TP-LINK®

450M 双频千兆无线路由器

TL-WR2543N

详细配置指南

Rev: 1.0.0

1910040214

声明

本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。除非有特殊约定，本手册仅作为使用指导，本手册中的所有陈述、信息等均不构成任何形式的担保。

目 录

第1章 详细配置指南简介

本文档旨在帮助您正确使用路由器的功能，内容包括路由器的性能特征以及所有功能的详细说明。若要使用路由器中的其他应用方面的功能，可以参考本文档相关部分内容。

1.1 本书约定

1. 用“→”符号说明在 WEB 界面上的操作引导，其方法是点击菜单、选项、按钮等。
2. 路由器配置界面的菜单或按钮名采用“加粗”字表示，其它选项名或操作项等用“”表示。
3. 图片界面都配有相关参数，这些参数主要是为正确配置产品参数提供参考。实际产品的配置界面并没有提供，请根据实际需要设置这些参数。

1.2 本书章节安排

第一章：详细配置指南简介。介绍本文档结构和编写约定。

第二章：产品概述。介绍路由器及其特性。

第三章：硬件描述。介绍路由器的前后面板以及安装环境注意事项。

第四章：快速安装指南。介绍硬件连接方法，并设置相关参数实现共享上网。

第五章：配置指南。介绍路由器包含的功能，请根据需要查看相关部分内容。

- WPS 一键安全设定：若您购买的 802.11n 无线网卡支持 WPS，可以通过 WPS 安全设置与网卡进行更为便捷和安全的无线连接。
- 网络参数：设置路由器的 LAN、WAN 口参数。LAN 口参数决定了计算机的 IP 地址，正确设置计算机 IP 地址才能访问路由器；WAN 口参数直接影响能否正常上网，请根据网络服务提供商提供的参数正确设置。
- 无线设置：设置路由器的无线参数。只有当网卡的参数和路由器的参数相匹配时，才能正常使用无线功能访问路由器；同时，通过此功能给无线网络加密可以防止他人非法入侵无线网络。
- DHCP 服务器：此功能可以自动为计算机分配 IP 地址，无须手动设置计算机的 IP 地址。
- 网络共享：使用此功能可方便地在局域网中共享 USB 存储设备上的卷。
- 转发规则：将计算机设置成网络服务器后，请配置此功能以保证网络中的其他用户可以访问您的服务器。
- 安全功能：此功能可以限制外网向局域网发起的连接、抑制局域网的泛洪攻击，并可以设置路由器的 LAN、WAN 口的管理权限。
- 家长控制：此功能可以管理小孩上网的时间和权限，为小孩的健康和学习提供保障。
- 上网控制：此功能可以管理局域网用户的上网时间和权限。

- 路由功能：对网络拓扑充分了解后，使用此功能可以减少路由选路造成的网络开销，提高数据包的转发速度。
- IP 带宽控制：此功能可以对局域网计算机上网带宽进行分配和控制，利用有限的带宽资源来保证重要数据及时传输。
- IP 与 MAC 绑定：此功能可以有效防止 ARP 攻击，维护局域网用户的上网安全。
- 动态 DNS：此功能可以使互联网主机通过域名访问路由器或局域网中的服务器。
- 系统工具：此部分为维护路由器的系统操作工具，可以对路由器进行升级，查看路由器的配置信息，同时当设置路由器出错时，可通过恢复出厂设置来重新设置。

附录 A　FAQ：解决配置路由器过程中的常见问题。

附录 B　IE 浏览器设置：介绍如何设置 IE 浏览器，保证正常访问路由器和上网。

附录 C　MAC 地址查询：介绍如何查看本机的 MAC 地址。

附录 D　规格参数：查看路由器的详细规格参数。

第2章 产品概述

2.1 产品简介

为了充分利用该款路由器的各项功能，请仔细阅读该详细配置指南。

TL-WR2543N 450M 双频千兆无线路由器提供最高达 1000 Mbps 的有线传输速率、450Mbps 的无线传输速率。它基于 IEEE 802.11n 标准，能扩展无线网络范围，同时兼容 IEEE 802.11a、IEEE 802.11b 和 IEEE 802.11g 标准，功能实用、性能优越、易于管理并且提供多重安全防护措施，可以有效保护用户的无线上网安全，满足小型企业、办公室和家庭办公室的无线上网需要。

2.2 主要特性

- 提供一个 10/100/1000Mbps 以太网(WAN)接口，可接 xDSL Modem/Cable Modem/Ethernet
- 内部集成四口交换机，提供四个 10/100/1000Mbps 以太网(LAN)接口
- 提供一个 USB 接口，可接 USB 存储设备，实现网络存储共享功能
- 支持最高达 1000Mbps 的有线传输速率
- 支持最高达 450Mbps 的无线传输速率，具备速率自适应功能，可以自动调整无线传输速率
- 支持 64/128/152 位 WEP 加密，WPA/WPA2、WPA-PSK/WPA2-PSK 等加密与安全机制，可以保证数据在无线网络传输中的安全
- 频段设置为 2.4GHz 时，可支持 11b only、11g only、11n only、11bg mixed 和 11bgn mixed 等多种无线模式；频段设置为 5GHz 时，可支持 11a only、11n only 和 11an mixed 多种无线模式。
- 支持 SSID 广播控制，有效防止 SSID 广播泄密
- 内置网络地址转换(NAT)功能，支持虚拟服务器、特殊应用程序和 DMZ 主机
- 内建 DHCP 服务器，同时可进行静态地址分配
- 支持 VPN 穿透
- 支持通用即插即用(UPnP)，符合 UPnP 标准的数据可顺利通过
- 内置安全功能，支持家长控制，可以有针对地开放指定计算机的上网权限
- 支持动态 DNS 功能，能够为动态 IP 地址提供域名服务
- 内置静态路由功能，可以根据需要构建特殊网络拓扑
- 支持基于 MAC 地址的局域网 WEB 管理，可以有效地限制局域网中计算机对 WEB 管理页面的访问

- 支持 WEB 软件升级，可以免费获得路由器的最新软件
- 可以根据上网动作，自动或按时连通和断开网络连接
- 支持本地和远端 WEB 管理
- 支持 WPS 快速安全设置

第3章 硬件描述

3.1 面板布置

3.1.1 前面板



图 3-1 TL-WR2543N 前面板示意图

指示灯：

指示灯	描述	功能
	电源指示灯	常灭－没有上电 常亮－已经上电
2.4GHz	2.4GHz 无线状态指示灯	常灭－没有启用 2.4GHz 无线功能 闪烁－已经启用 2.4GHz 无线功能
5GHz	5GHz 无线状态指示灯	常灭－没有启用 5GHz 无线功能 闪烁－已经启用 5GHz 无线功能
1-4	局域网状态指示灯	常灭－相应端口没有连接上 常亮－相应端口已正常连接 闪烁－相应端口正在进行数据传输
	广域网状态指示灯	常灭－端口没有连接上 常亮－端口已正常连接 闪烁－端口正在进行数据传输
	USB 状态指示灯	常灭－端口没有连接上 常亮－端口已正常连接
	WPS 安全连接指示灯	慢闪－表示正在进行安全连接， 此状态持续约 2 分钟 慢闪转为常亮－表示安全连接成功 慢闪转为快闪－表示安全连接失败

☞ 注意：

1. 正常状态下，2.4GHz 无线状态指示灯和 5GHz 无线状态指示灯之一为闪烁，另一指示灯为常灭。
2. 安全连接成功后，WPS 指示灯的常亮状态约持续 5 分钟后会自动熄灭，此种状态仍然属于正常连接状态。

3.1.2 后面板

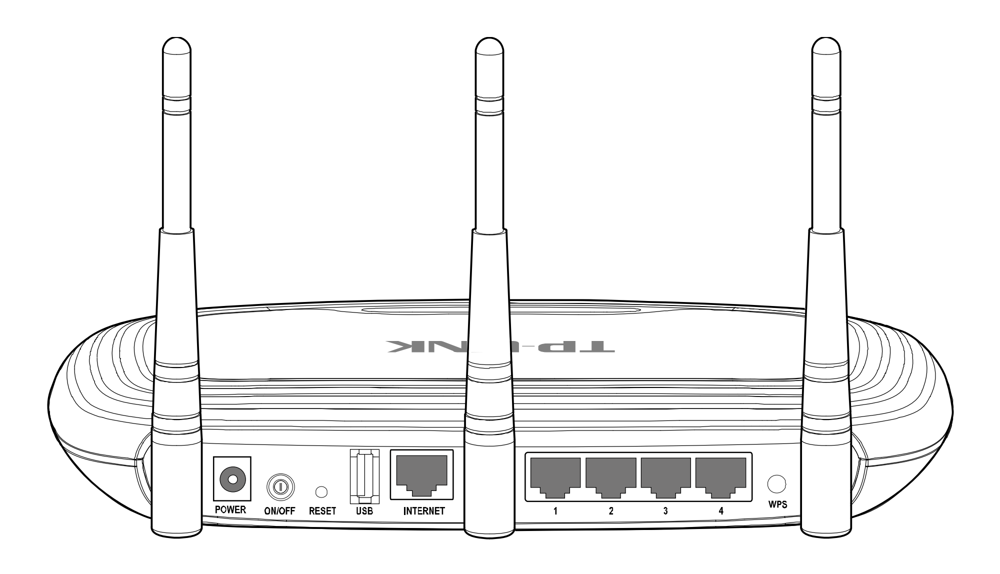


图 3-2 TL-WR2543N 后面板示意图

POWER： 电源插孔，用来连接电源，为路由器供电。

☞ 注意：

为了保证设备正常工作，请使用额定电源。

ON/OFF： 电源开关。

RESET： 复位按钮。用来使设备恢复到出厂默认设置。

USB： USB 设备插孔。该端口用来连接局域网中的 USB 存储设备，实现网络存储及共享功能。

INTERNET：广域网端口插孔(RJ45)。该端口用来连接以太网电缆或 xDSL Modem/Cable Modem（即"猫"）。

1/2/3/4： 局域网端口插孔(RJ45)。该端口用来连接局域网中的集线器、交换机或安装了网卡的计算机。

天线： 用于无线数据的收发。

3.2 复位

如果要将路由器恢复到出厂默认设置，请在路由器通电的情况下按压 RESET 按钮，大约等待五秒钟，直到所有指示灯均为灭，此时路由器已成功恢复出厂设置，松开 RESET 按钮，路由器将重启。

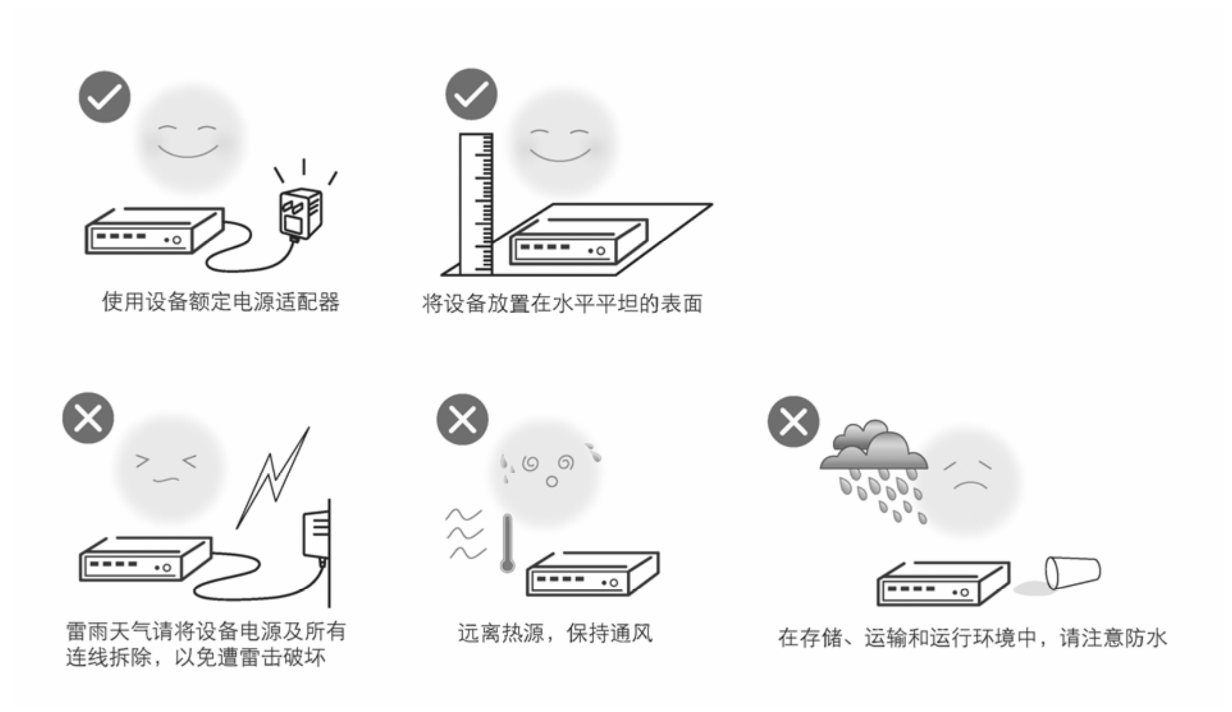
3.3 系统需求

- 宽带 Internet 服务(接入方式为以太网电缆接入或通过 xDSL/Cable Modem 接入)
- 具有 RJ45 口的调制解调器(直接使用以太网电缆接入时不需要此设备)

- 每台 PC 的以太网连接设备(无线网卡或有线网卡及网线)
- 支持 TCP/IP 协议的操作系统
- Web 浏览器，如 Microsoft Internet Explorer、Mozilla Firefox、Apple Safari 等

3.4 安装环境

该路由器安装时应该遵循以下原则：



☞ 注意：

环境因素对传输距离有影响，详细介绍见附录A。

第4章 快速安装指南

本章介绍如何连接路由器并成功实现多台计算机共享上网。如果只进行基本配置，只需阅读本章内容；如果要进行高级配置，请继续阅读第 5 章内容。

4.1 硬件连接

在安装路由器前，我们希望您已经能够利用宽带服务在单台计算机上成功上网。如果单台计算机上网有问题，请先和网络服务商（ISP）联系解决问题。成功地利用单台计算机上网后，请遵循以下步骤安装路由器。安装时请拔除电源插头，保持双手干燥。

1. 建立局域网连接

用网线将计算机直接连接到路由器LAN口。也可以将路由器的LAN口和局域网中的集线器或交换机通过网线相连，如下图 4-1所示。

2. 建立广域网连接

用网线将路由器Internet口和xDSL/Cable Modem或以太网相连，如下图 4-1所示。

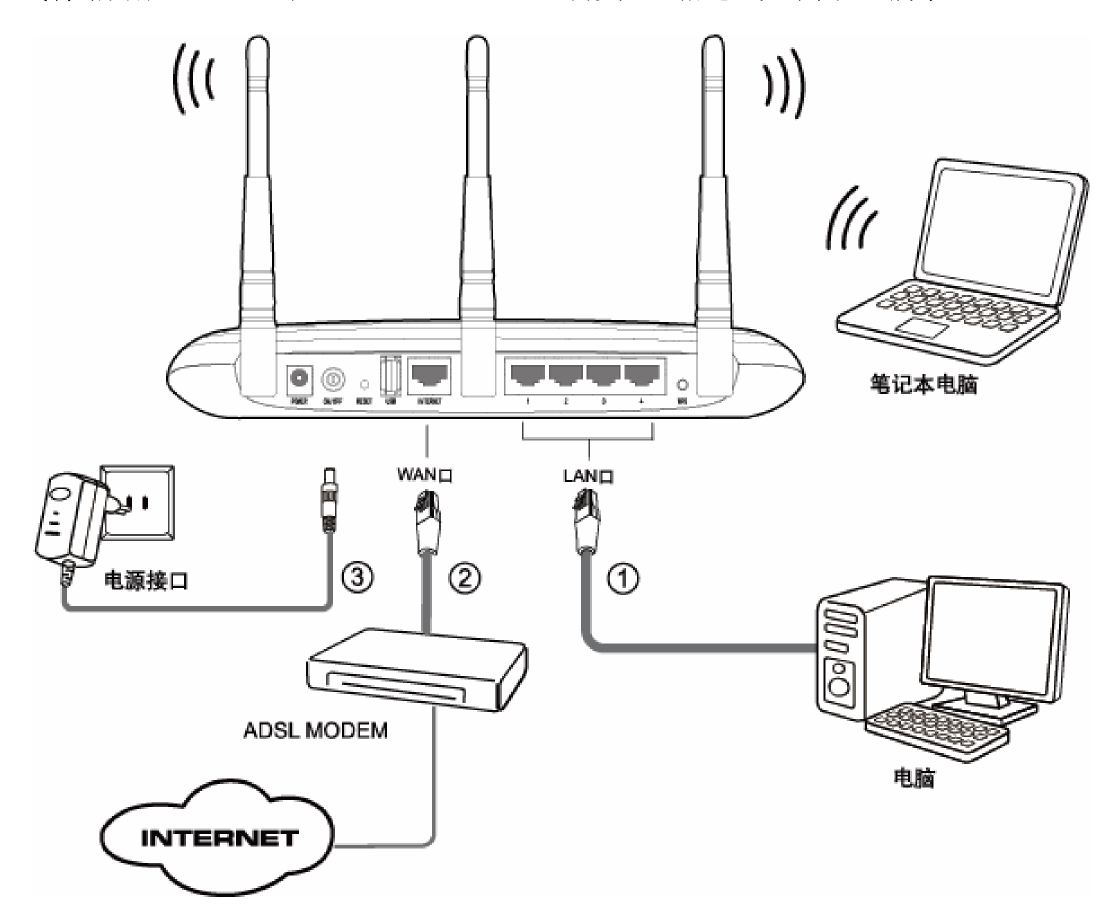


图 4-1 TL-WR2543N 硬件安装示意图

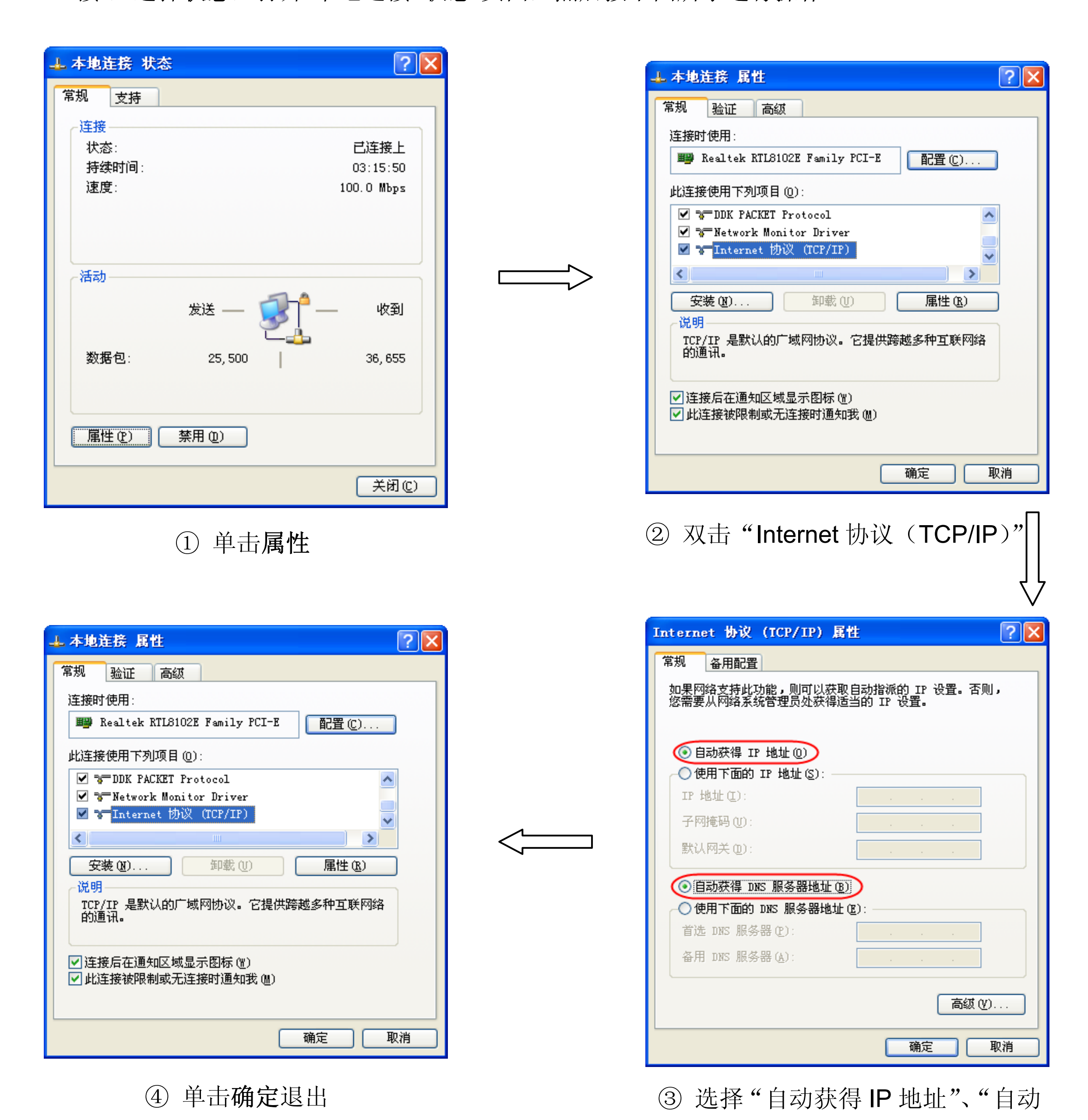
3. 连接电源

连接好电源，然后按下 ON/OFF 电源开关，路由器将自行启动。

4.2 建立正确的网络设置

本路由器默认 LAN 口 IP 地址是 192.168.1.1，默认子网掩码是 255.255.255.0。这些值可以根据实际需要而改变，但本手册中将按默认值说明。本节以 Windows XP 系统为例，介绍计算机参数的设置步骤。

1. 右键单击桌面上的“网上邻居”图标，选择**属性**，在打开的“网络连接”页面中，右键单击“本地连接”，选择**状态**，打开“本地连接 状态”页面，然后按下图所示进行操作。



① 单击**属性**

② 双击“Internet 协议（TCP/IP）”

③ 选择“自动获得 IP 地址”、“自动获得 DNS 服务器地址”，单击**确定**

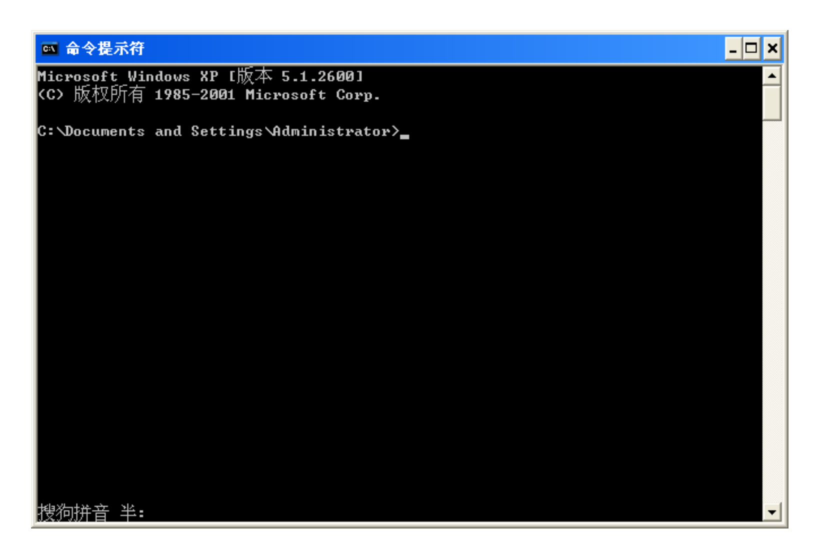
④ 单击**确定**退出

提示：

Windows 98 或更早版本的操作系统，以上设置可能需要重启计算机。

2. 使用 Ping 命令检查计算机和路由器之间是否连通。在 Windows XP 环境中，点击**开始－运行**，

在随后出现的运行窗口输入“cmd”命令，回车或点击**确定**进入下图所示界面。



3. 输入命令：Ping 192.168.1.1，回车。

如果屏幕显示为：

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

说明计算机已与路由器成功建立连接。

如果屏幕显示为：

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

这说明设备还未安装好，请按照下列顺序检查：

1) 硬件连接是否正确？

路由器面板上对应局域网端口的1-4局域网状态指示灯（指示各端口的 Link/Act 状态）和计算机上的网卡指示灯必须亮。

2) 计算机的 TCP/IP 设置是否正确？

若计算机的 IP 地址为前面介绍的自动获取方式，则无须进行设置。若手动设置 IP，请注意如果路由器的 IP 地址为 192.168.1.1，那么计算机 IP 地址必须为 192.168.1.X（X 是 2 到 254 之间的任意整数），子网掩码须设置为 255.255.255.0，默认网关须设置为 192.168.1.1。

4.3 快速安装指南

本产品提供基于 WEB 浏览器的配置工具，可以在任何基于 Windows，Macintosh 或 UNIX 平台的 WEB 浏览器（如 Microsoft Internet Explorer、Mozilla Firefox、Apple Safari 等）中使用该配置工具配置路由器。

为了顺利通过本路由器连接互联网，首先请设置WEB浏览器，具体设置步骤请参阅附录B IE浏览器设置。

打开网页浏览器，在浏览器的地址栏中输入路由器的IP地址：192.168.1.1，可以看到下图 4-2所示登录界面，输入用户名和密码（用户名和密码的出厂默认值均为admin），单击**确定**按钮。



图 4-2 登录界面

浏览器会弹出如下图 4-3所示的设置向导页面。如果没有自动弹出此页面，可以单击页面左侧的**设置向导**菜单将它激活。

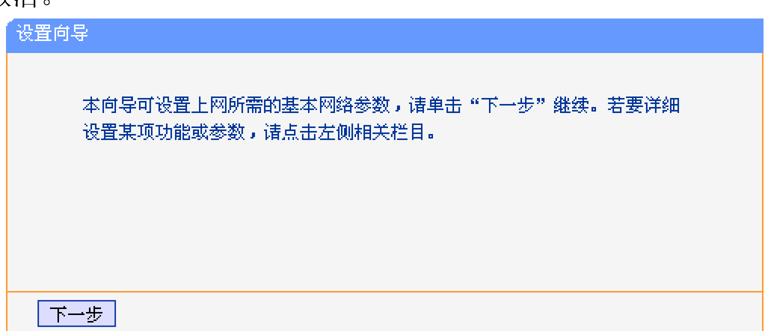


图 4-3 设置向导

单击**下一步**，进入下图 4-4所示的上网方式选择页面。

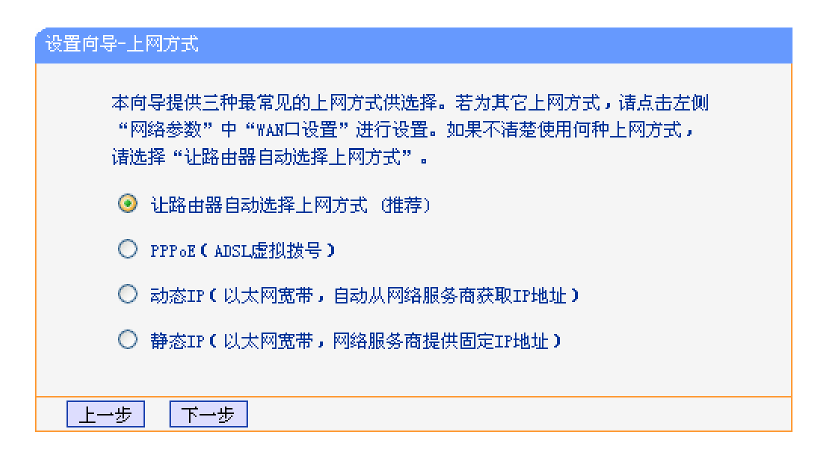


图 4-4 设置向导——上网方式

图 4-4显示了最常用的几种上网方式，请根据ISP提供的上网方式进行选择，然后单击下一步填写ISP提供的网络参数。

➢ 让路由器自动选择上网方式（推荐）

选择该选项后，路由器会自动判断上网类型，然后跳到相应上网方式的设置页面。为了保证路由器能够准确判断上网类型，请保证路由器已正确连接。

➢ PPPoE（ADSL 虚拟拨号）

如果您的上网方式为PPPoE，即ADSL虚拟拨号方式，ISP会提供上网帐号和口令，这时需要在下图4-5所示页面中输入ISP提供的ADSL上网帐号和口令。

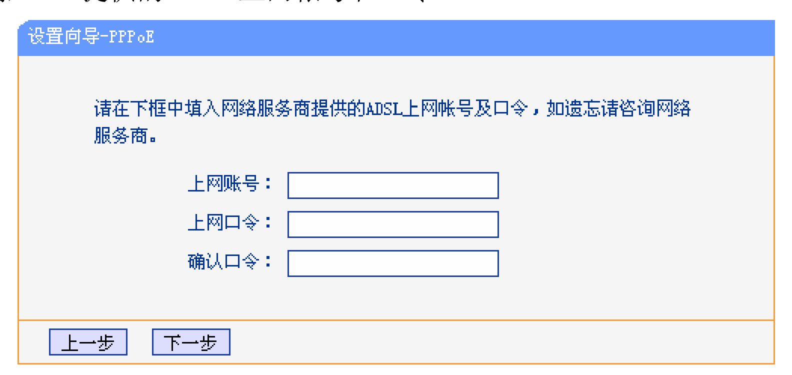


图 4-5 上网方式——PPPoE

➢ 动态IP（以太网宽带，自动从网络服务商获取IP地址）

如果您的上网方式为动态IP，则可以自动从网络服务商获取IP地址，无须做任何设置。单击下一步转到图 4-7进行无线参数的设置。

➢ 静态 IP（以太网宽带，网络服务商提供固定 IP 地址）

如果您的上网方式为静态IP，网络服务商会提供IP地址参数，您需要在下图 4-6所示页面中输入ISP提供的参数，若有不明白的地方请咨询网络服务商。



图 4-6 上网方式——静态 IP

IP 地址： 本路由器对广域网的 IP 地址，即 ISP 提供的 IP 地址，不清楚可以向 ISP 询问。

子网掩码： 本路由器对广域网的子网掩码，即 ISP 提供的子网掩码，一般为 255.255.255.0。

网关： 填入 ISP 提供的网关参数，不清楚可以向 ISP 询问。

DNS 服务器： 填入 ISP 提供的 DNS 服务器地址，不清楚可以向 ISP 询问。

备用 DNS 服务器：

可选项，如果 ISP 提供了两个 DNS 服务器地址，则可以把另一个 DNS 服务器地址的 IP 地址填于此处。

设置完成后，单击**下一步**，可以看到下图 4-7所示的基本无线网络参数设置页面。

设置向导 - 无线设置

本向导页面设置路由器无线网络的基本参数以及无线安全。

无线状态： 开启

SSID： TP-LINK_DE1C2E

频段： 2.4G

模式： 11bgn mixed

频段带宽： 自动

信道： 自动

最大发送速率： 450M

无线安全选项：

为保障网络安全，强烈推荐开启无线安全，并使用WPA-PSK/WPA2-PSK AES加密方式。

不开启无线安全

WPA-PSK/WPA2-PSK

PSK密码：

（8-63个ASCII码字符或8-64个十六进制字符）

不修改无线安全设置

上一步 下一步

图 4-7 设置向导——无线设置

无线状态： 开启或者关闭路由器的无线功能。

SSID： 设置任意一个字符串来标明您的无线网络。

频段： 设置无线数据传输时所占用的频段，可选项有 2.4GHz 和 5GHz。

模式： 设置路由器的无线工作模式。频段选为 2.4GHz 时，推荐使用 11bgn mixed 模式；频段选为 5GHz 时，推荐使用 11an mixed 模式。

频段带宽： 设置无线数据传输时所占用的信道宽度，可选项有 20MHz、40MHz 和自动。

信道： 设置路由器的无线信号频段，推荐选择自动。

最大发送速率： 设置路由器无线网络的最大发送速率。

不开启无线安全： 关闭无线安全功能，即不对路由器的无线网络进行加密，此时其他人均可以加入您的无线网络。

WPA-PSK/WPA2-PSK：

路由器无线网络的加密方式，如果选择了该项，请在 PSK 密码中输入想要设置的密码，密码要求为 8-63 个 ASCII 字符或 8-64 个 16 进制字符。

不修改无线安全设置：

选择该项，则无线安全选项中将保持上次设置的参数。

☞ 注意：

1. 以上提到的频段带宽设置仅针对支持 IEEE 802.11n 协议的无线网络设备，对于不支持 IEEE 802.11n 协议的设备，此设置不生效。
2. 若您的终端设备不支持 5GHz 频段，而路由器的频段设置为 5GHz，则该终端设备将无法搜索到路由器的无线信号。

设置完成后，单击**下一步**，如果更改了无线设置，将弹出下图 4-8所示的设置向导完成界面，单击**重启**使无线设置生效。如果没有更改无线设置，将弹出下图 4-9所示的设置向导完成界面，单击**完成**结束设置向导。

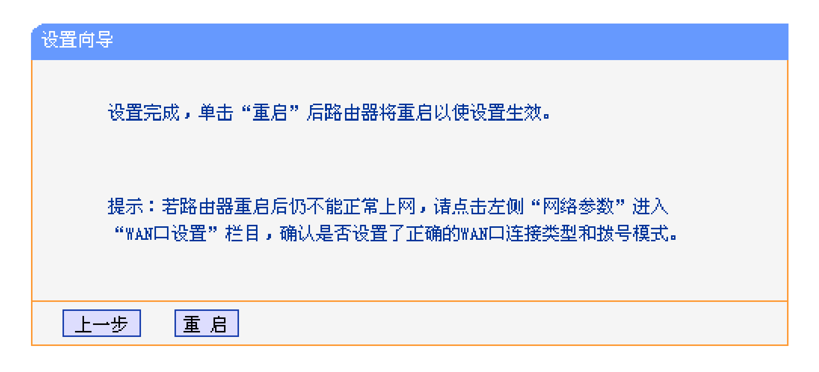


图 4-8 设置完成——重启使设置生效

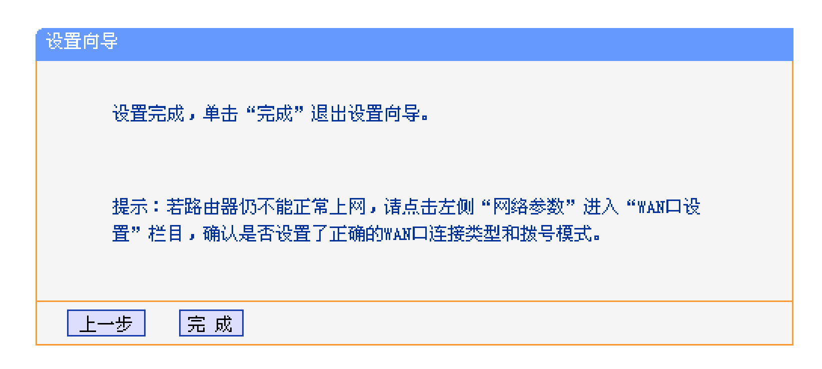


图 4-9 设置完成——结束设置向导

第5章 配置指南

5.1 启动和登录

启动路由器并成功登录路由器管理页面后，浏览器会显示设置向导界面，如图 5-1。

在左侧菜单栏中，共有如下几个菜单：运行状态、设置向导、WPS 一键安全设定、网络参数、无线设置、DHCP 服务器、网络共享、转发规则、安全功能、家长控制、上网控制、路由功能、IP 带宽控制、IP 与 MAC 绑定、动态 DNS 和系统工具。单击某个菜单项，即可进行相应的功能设置。下面将详细讲解各个菜单的功能。



图 5-1 启动和登录

5.2 运行状态

选择菜单**运行状态**，可以查看路由器当前的状态信息，包括版本信息、WAN口状态、LAN口状态、无线状态和WAN口流量统计信息，如图 5-2。

版本信息

当前软件版本：	3.13.12 Build 120109 Rel.35902n
当前硬件版本：	WR2543N v1 00000000

WAN口状态

MAC地址：	DE-AD-C0-DE-1C-2F	
IP地址：	0.0.0.0	动态IP
子网掩码：	0.0.0.0	
默认网关：	0.0.0.0	更新
DNS服务器：	0.0.0.0 , 0.0.0.0	

LAN口状态

MAC地址：	DE-AD-C0-DE-1C-2E
IP地址：	192.168.1.1
子网掩码：	255.255.255.0

无线状态

无线功能：	开启
SSID号：	TP-LINK_DE1C2E
频段：	2.4G
模式：	11bgn mixed
信道：	自动 (当前信道 9)
频段带宽：	自动
最大发送速率：	450Mbps
MAC地址：	DE-AD-C0-DE-1C-2E
WDS状态：	未开启

流量统计

	接收	发送
字节数：	0	0
数据包数：	0	0

运行时间： 0 天 00:00:53 刷新

图 5-2 运行状态

版本信息： 此处显示路由器当前的软硬件版本号。可以在**系统工具→软件升级**界面升级软件版本。

WAN 口状态： 此处显示路由器当前 WAN 口的 MAC 地址、IP 地址、子网掩码、网关和 DNS 服务器地址。可以在**网络参数→WAN 口设置**界面中进行相关设置。

LAN 口状态： 此处显示路由器当前LAN口的MAC地址、IP地址和子网掩码。其中IP地址和子网掩码可以在**网络参数→LAN口设置**界面中进行设置。

无线状态： 此处显示路由器当前的无线设置状态，包括 SSID、信道和频段带宽等信息。可以在**无线设置→基本设置**界面进行相关设置。

5.3 设置向导

详见4.3 快速安装指南。

5.4 WPS一键安全设定

选择菜单**WPS一键安全设定**，可以在下图 5-3界面中进行快速无线安全设置。

WPS一键安全设定

WPS 功能：已开启 关闭WPS

当前PIN码：96020784 恢复初始PIN码 产生新的PIN码

添加新设备： 添加设备

帮 助

图 5-3 WPS 一键安全设定

WPS 功能： WPS 即快速安全设置，使用该功能可以快速建立与无线网卡之间的无线连接。默认状态为开启。

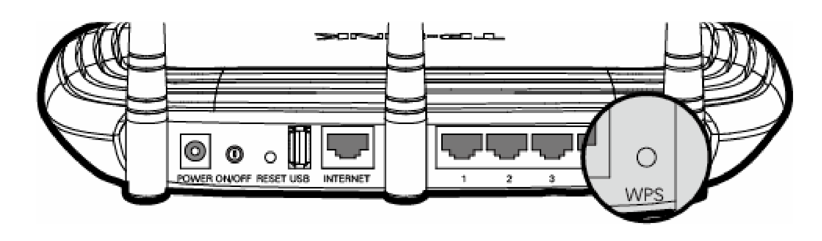
当前PIN码： PIN码即个人识别码，用于标识一件无线产品。PIN码可以更改，如果目前使用的PIN码与他人重复，可以点击**产生新的PIN码**，也可以点击**恢复初始PIN码**返回到最初PIN码值，恢复初始PIN码或者产生新的PIN码，都必须重启路由器后才能生效。

添加新设备： 点击**添加设备**进入添加新设备界面，在此界面可以通过手动配置路由器，添加要与其进行连接的无线设备。

WPS（WiFi Protected Setup）能够快速建立与无线网卡之间的安全连接。如果您现在拥有支持 QSS 的无线网卡，以我司 TL-WN821N 的 11N 无线 USB 网卡为例，可以通过下面任意一种方法快速组建安全的无线网络：

方法一：

1. 按下路由器面板上的WPS快速安全按钮。



2. 接着按下网卡上的QSS快速安全按钮2到3秒不放。



3. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。

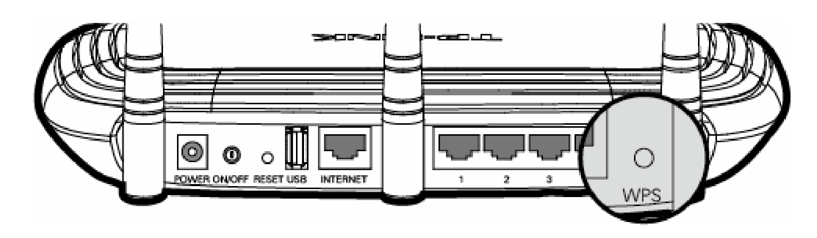


4. 出现下图所示界面则表示网卡端快速安全连接配置成功，单击**完成**结束配置。

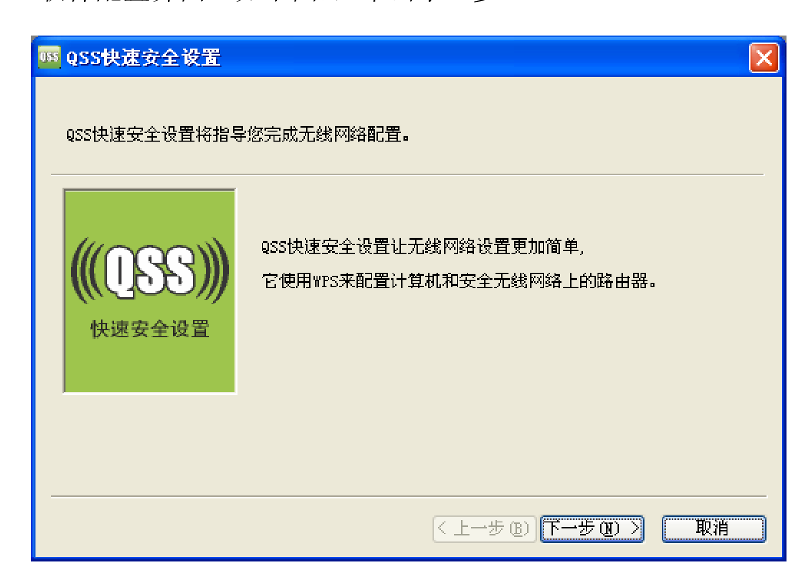


方法二：

1. 按下路由器面板上的WPS快速安全按钮。



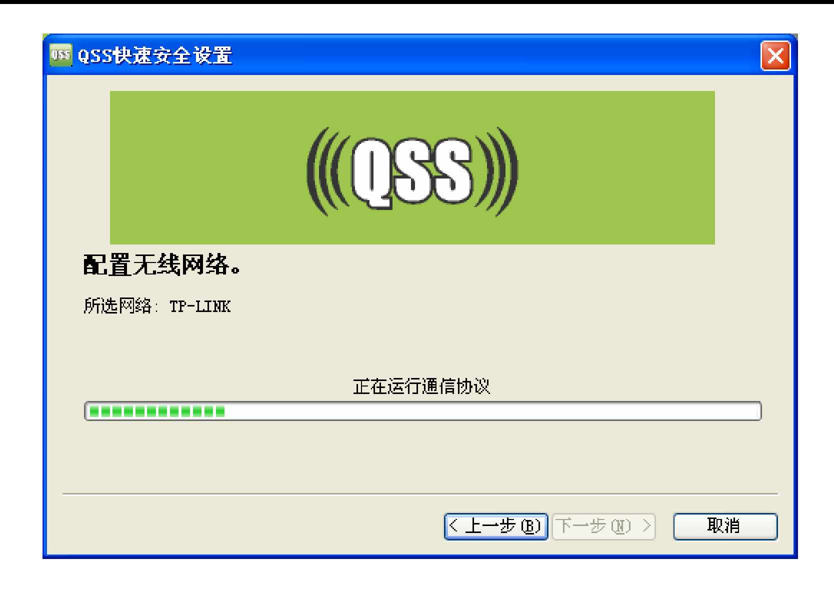
2. 进入网卡QSS软件配置界面（如下图），单击下一步。



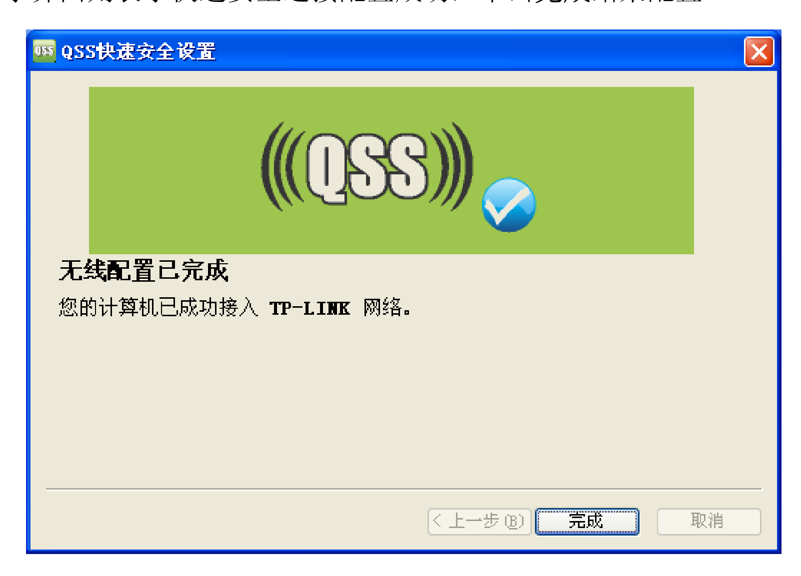
3. 在随后出现的如下图所示的界面中选择第一项，单击下一步。



4. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。



5. 出现下图所示界面则表示快速安全连接配置成功，单击**完成**结束配置。



方法三：

1. 进入本路由器管理界面，在“WPS 一键安全设定”界面中（如下图）选择**添加设备**。



2. 在随后出现的如下图所示的界面中选择“按下新设备上的按钮”，然后点击**连接**按钮。

添加新的设备

输入准备添加的新设备的PIN码。

PIN码：

按下新设备上的按钮。

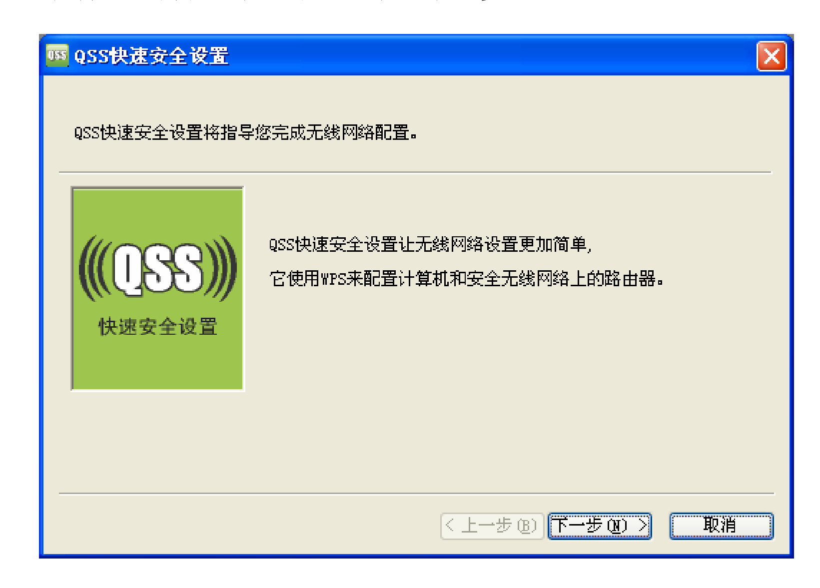
返回 连接

帮 助

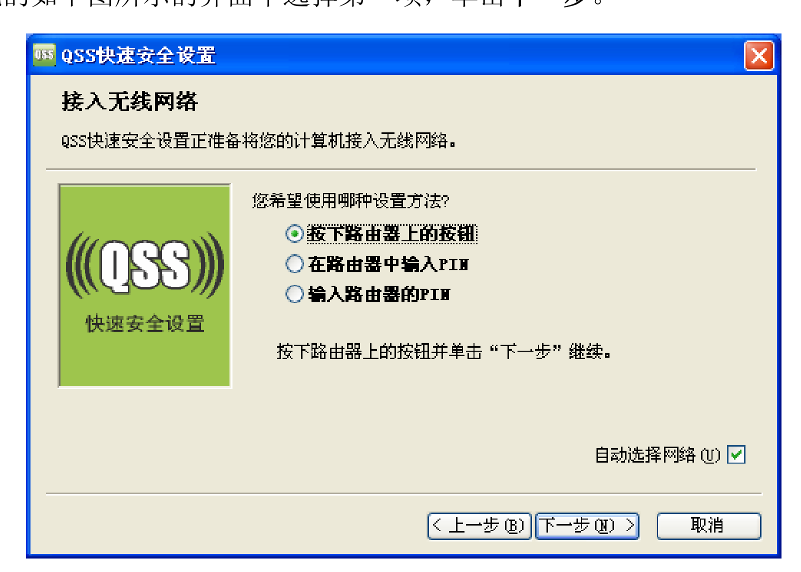
☞ 注意：

上述操作步骤 2 等同于按下路由器面板上的 WPS 快速安全按钮。

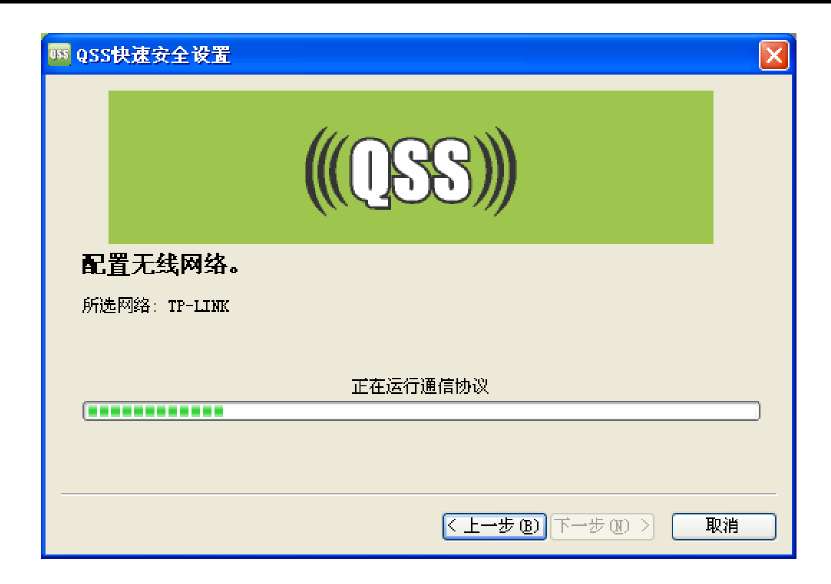
3. 进入网卡QSS软件配置界面（如下图），单击**下一步**。



4. 在随后出现的如下图所示的界面中选择第一项，单击**下一步**。



5. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。



6. 出现下图所示界面则表示网卡端快速安全连接配置成功，单击**完成**结束配置。

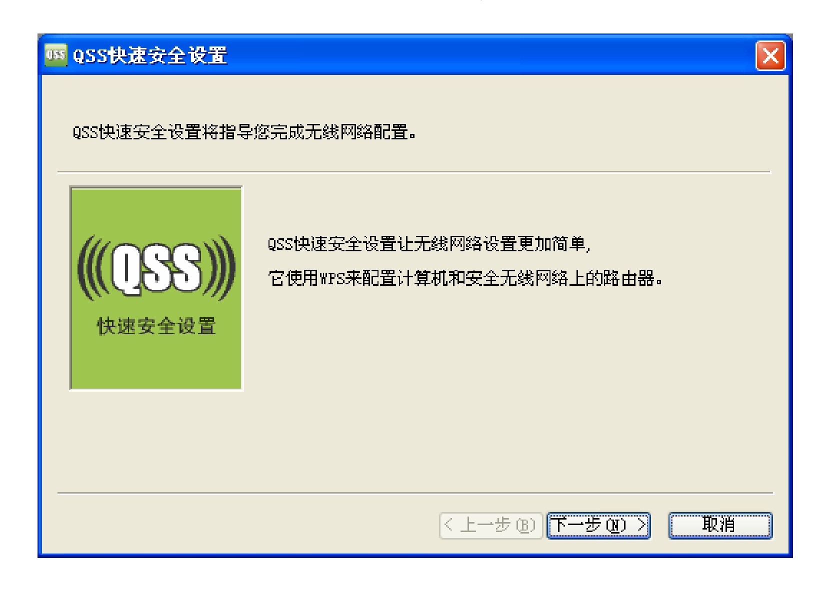


此时路由器端 WPS 一键安全设定的“添加新的设备”界面显示“添加设备成功”。



方法四：

1. 进入网卡QSS软件配置界面（如下图），单击下一步。



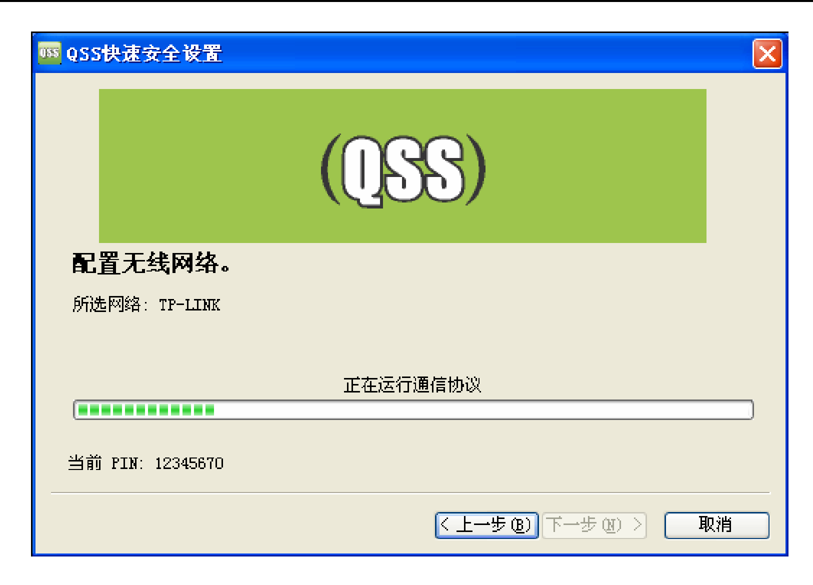
2. 在随后出现的如下图所示的界面中选择最后一项，并在"路由器 PIN"后面的方框中输入路由器底部标贴上的 8 位 PIN 码，单击下一步。

☞ 注意：

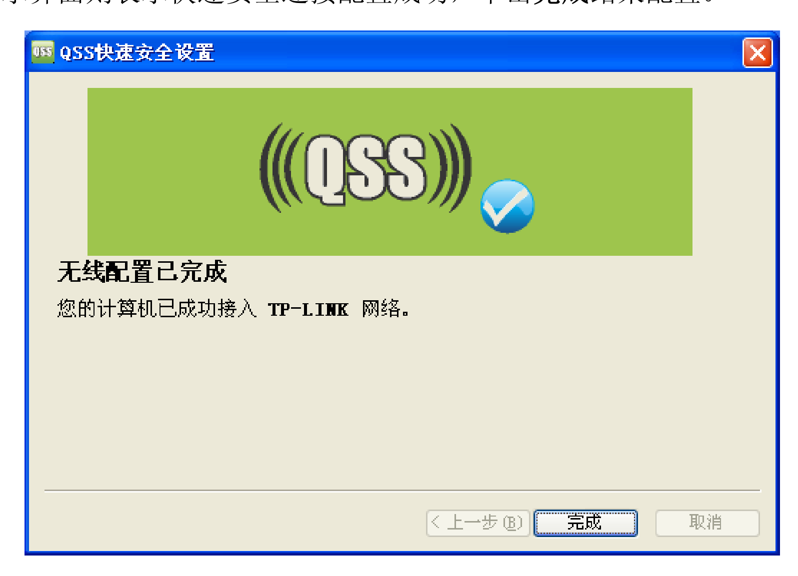
如果路由器已经有新的 PIN 码时，请在路由器管理界面的"WPS 安全设置"界面中读取当前 PIN 码填在下图中的"路由器 PIN"后面的方框中。



3. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。

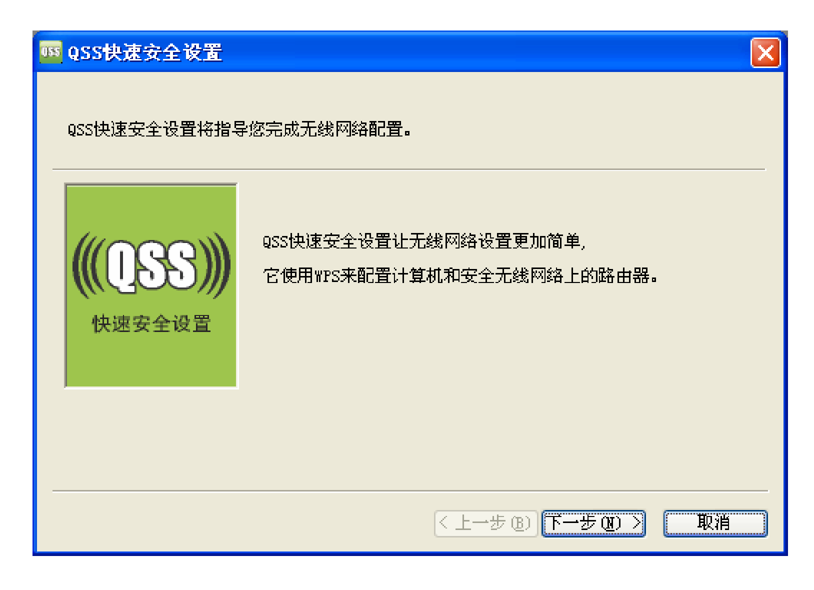


4. 出现下图所示界面则表示快速安全连接配置成功，单击**完成**结束配置。



方法五：

1. 进入网卡QSS软件配置界面（如下图），单击**下一步**。



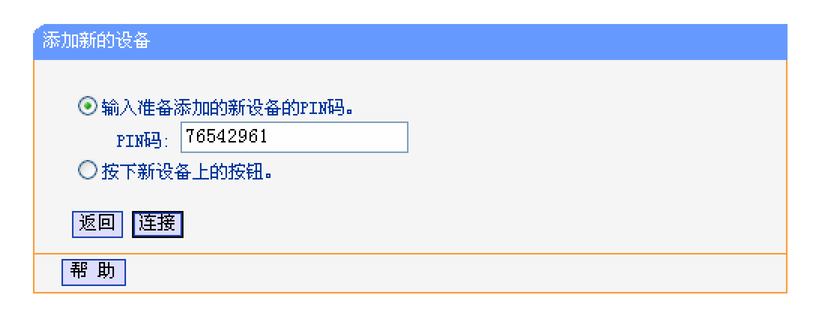
2. 在随后出现的如下图所示的界面中选择第二项，记录粗体显示的8位数字，这便是网卡的PIN码。然后单击**下一步**。



3. 进入本路由器管理界面，在"WPS 一键安全设定"界面中选择**添加设备**。



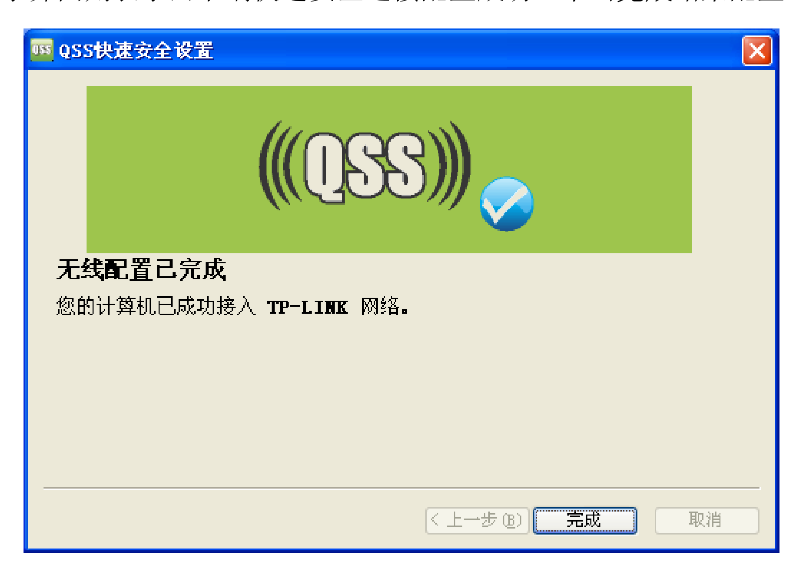
4. 在随后出现的如下图所示的界面中选择"输入准备添加的新设备的 PIN 码"，在下方的 PIN 码框中输入在第 2 步记录的 8 位网卡 PIN 码，然后点击**连接**按钮。



5. 接下来是网卡与路由器建立无线安全网络的过程，请稍作等待。



6. 出现下图所示界面则表示网卡端快速安全连接配置成功，单击**完成**结束配置。



此时路由器端 WPS 一键安全设定的“添加新的设备”界面会显示“添加设备成功”。



5.5 网络参数

在网络参数功能中，可以根据组网需要设置路由器在局域网中的 IP 地址，并根据 ISP 提供的网络参数方便快捷地设置路由器 WAN 口参数，使局域网计算机能够共享 ISP 提供的网络服务。

选择菜单**网络参数**，可以看到：

- 网络参数
  - WAN口设置
  - LAN口设置
  - MAC地址克隆

单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.5.1 WAN口设置

WAN 是广域网(Wide Area Network)的缩写。在对 WAN 口参数的设置中，可以根据 ISP 提供的连接类型方便快捷地设置路由器，使局域网计算机共享 ISP 提供的网络服务。在此设置中各种参数均由 ISP 提供，当参数不明确时请咨询 ISP。

选择菜单**网络参数→WAN口设置**，可以在随后出现的界面中配置WAN口的网络参数。本路由器支持6种上网方式：动态IP、静态IP、PPPoE、L2TP、PPTP和DHCP+，请咨询 ISP 提供哪种上网方式同时提供相关参数。

1. 动态 IP

当ISP未提供任何IP网络参数时，请选择**动态IP**。如图 5-4 WAN口设置-动态IP所示。选择**动态IP**，路由器将从ISP自动获取IP地址。

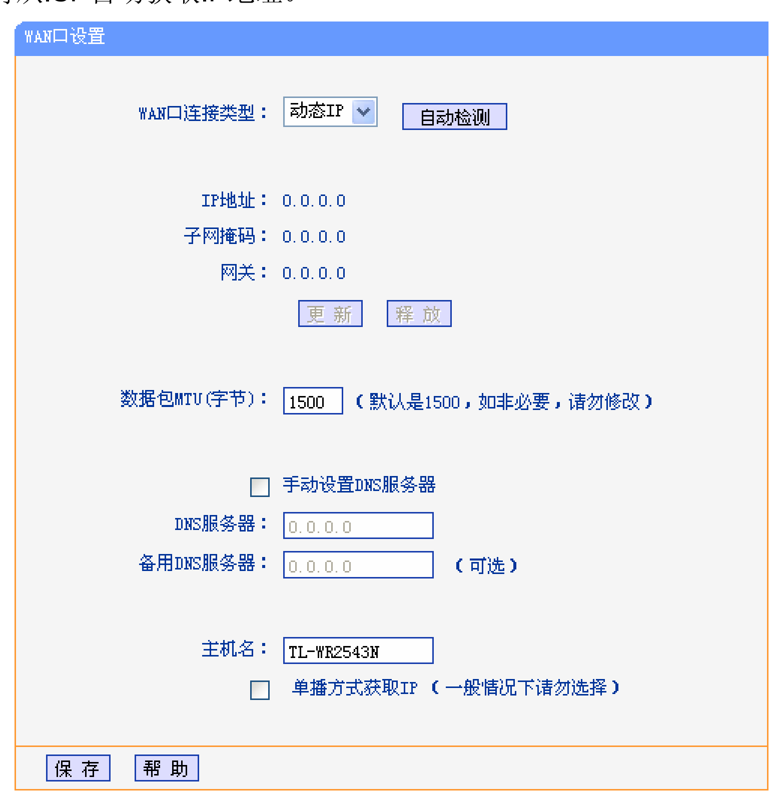


图 5-4 WAN 口设置-动态 IP

自动检测： 点击**自动检测**按钮，路由器能检测动态IP、静态IP和PPPoE三种上网方式，检测结果仅供参考，确切的上网方式请咨询ISP。

更新： 单击**更新**按钮，可以查看路由器从ISP的DHCP服务器上动态得到IP地址、子网掩码、网关以及DNS服务器。

释放： 单击**释放**按钮，路由器将发送DHCP释放请求给ISP的DHCP服务器，释放IP地址、子网掩码、网关以及DNS服务器设置。

数据包MTU： MTU全称为最大数据传输单元，缺省为1500。请向ISP咨询是否需要更改。如非特别需要，一般不要更改。

DNS服务器、备用DNS服务器：

显示从ISP处自动获取的DNS服务器地址。当您需要使用已有的DNS服务器时，勾选“手动设置DNS服务器”，并在此处输入DNS服务器和备用DNS服务器(选填)的IP地址。路由器将优先连接手动设置的DNS服务器。

单播方式获取IP： 少数ISP的DHCP服务器不支持广播请求方式，如果在网络连接正常的情况下无法获取IP地址，请选择此项。

完成更改后，点击**保存**按钮。

2. 静态 IP

当ISP提供的上网方式为静态IP时，ISP会给您提供上网帐号和上网口令。IP地址、子网掩码、网关和DNS服务器等WAN IP信息时，请选择**静态IP**。如图 5-5 WAN口设置-静态IP所示。具体设置时，若不清楚，请咨询ISP。

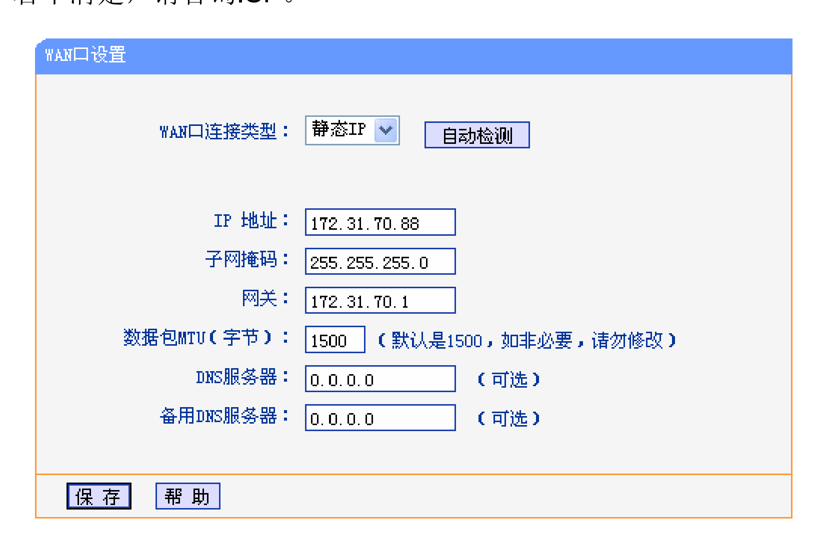


图 5-5 WAN 口设置-静态 IP

自动检测： 点击**自动检测**按钮，路由器能检测动态IP、静态IP和PPPoE三种上网方式，检测结果仅供参考，确切的上网方式请咨询ISP。

IP地址： 输入ISP提供的IP地址信息，必填项。

子网掩码： 输入ISP提供的子网掩码，必填项。根据不同的网络类型子网掩码不同，一般为255.255.255.0 (C类)。

网关： 输入ISP提供的网关参数。

数据包MTU： MTU全称为最大数据传输单元，缺省为1500。请向ISP咨询是否需要更改。如非特别需要，一般不要更改。

DNS服务器、备用DNS服务器：

ISP一般至少会提供一个DNS(域名服务器)地址，若提供了两个DNS地址则将其中一个填入“备用DNS服务器”栏。

完成更改后，点击**保存**按钮。

3. PPPoE

如果ISP提供的上网方式是PPPoE(以太网上的点到点连接)，ISP会给您提供上网帐号和上网口令，请选择**PPPoE**。如图 5-6 WAN口设置-PPPoE。具体设置时，若不清楚，请咨询ISP。

WAN口设置
WAN口连接类型： PPPoE 自动检测
PPPoE连接：
上网账号：
上网口令：
确认口令：
特殊拨号： 自动选择拨号模式
第二连接： 禁用 动态IP 静态IP
根据您的需要，请选择对应的连接模式：
按需连接，在有访问时自动连接
自动断线等待时间： 15 分 （0 表示不自动断线）
自动连接，在开机和断线后自动连接
定时连接，在指定的时间段自动连接
注意：只有当您到“系统工具”菜单的“时间设置”项设置了当前时间后，“定时连接”功能才能生效。
连接时段：从 0 时 0 分到 23 时 59 分
手动连接，由用户手动连接
自动断线等待时间： 15 分 （0 表示不自动断线）
连 接 断 线 未连接
高级设置
保 存 帮 助

图 5-6 WAN 口设置-PPPoE

自动检测： 点击**自动检测**按钮，路由器能检测动态IP、静态IP和PPPoE三种上网方式，检测结果仅供参考，确切的上网方式请咨询ISP。

上网帐号： 请正确输入ISP提供的上网帐号，必须填写。

上网口令： 请正确输入ISP提供的上网口令，必须填写。

第二连接： 如果ISP还提供了以动态IP或静态IP的方式连接到局域网的连接，则可以相应地选择“动态IP”或“静态IP”来启动这个连接。

按需连接： 若选择按需连接模式，当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。对于采用按使用时间进行交费的用户，选择按需连接可以有效节省上网费用。

自动断线等待时间：

如果自动断线等待时间T不等于0(默认时间为15分钟)，则在检测到连续T分钟内没有网络访问流量时自动断开网络连接，保护您的上网资源。此项设置仅对“按需连接”和“手动连接”生效。

自动连接： 在开机后系统自动连接网络。在使用过程中，如果由于外部原因网络被断开，系统就会主动尝试连接，直到成功连接。若您的网络服务是包月交费形式，可以选择该项连接方式。

定时连接： 系统在连接时段的开始时刻主动进行网络连接，在终止时刻自动断开网络连接。选择此连接模式，可以有效控制内网用户的上网时间。

手动连接： 开机或断线后，需要在此处或个人计算机中手动拨号连接。若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若您的网络服务是按时间交费，选择手动连接可有效节省上网费用。

连接/断线： 单击此按钮，可进行即时的连接/断线操作。

若需要进一步设置，可以点击**高级设置**按钮，在图5-7 WAN口设置-PPPoE-高级设置界面中进行高级设置。

图 5-7 WAN 口设置-PPPoE-高级设置

数据包MTU： 填入网络数据包的MTU值，缺省为1480，如非特别需要，一般不要更改。

服务名、服务器名称：

如果不是ISP特别要求，请不要填写这两项。

使用ISP指定IP地址：

该项仅适用于静态PPPoE。如果ISP提供上网帐号和口令时，还提供了IP地址，请选中此选择框，并输入PPPoE连接的静态IP地址。

在线检测间隔时间：

设置该值后，路由器将根据指定的时间间隔发送检测信号，以检测服务器是否在线。如果该值为0，则表示不发送检测信号。

DNS服务器、备用DNS服务器：

该处显示从ISP处自动获得的DNS服务器地址。当需要使用已有的DNS服务器时，请选择"手动设置DNS服务器"，并手动输入DNS服务器和备用DNS服务器IP地址(至少设置一个)。连接时，路由器将优先使用手动设置的DNS服务器。

完成更改后，点击**保存**按钮。

4. L2TP

如果ISP提供的上网方式是L2TP，ISP会给您提供上网帐号和上网口令。具体设置时，若不清楚，请咨询ISP。见图 5-8 WAN口设置-L2TP。

WAN口设置

WAN口连接类型： L2TP

上网帐号： username

上网口令： ••••••••

连 接　断 线　未连接

动态 IP　静态 IP

服务器 IP /域名：

IP 地址： 0.0.0.0

子网掩码： 0.0.0.0

网关： 0.0.0.0

DNS： 0.0.0.0 , 0.0.0.0

Internet IP： 0.0.0.0

Internet DNS： 0.0.0.0 , 0.0.0.0

数据包MTU(字节)： 1460 （缺省值为1460，如非必要，请勿修改）

根据您的需要，请选择对应的连接模式：

自动断线等待时间： 15 分 （0 表示不自动断线）

按需连接，在有访问数据时自动进行连接

自动连接，在开机和断线后自动连接

手动连接，由用户手动连接

保 存　帮 助

图 5-8 WAN 口设置-L2TP

上网帐号： 请正确输入ISP提供的上网帐号，必须填写。

WAN口连接类型：

请根据您的Internet服务供应商(ISP)所提供的上网方式来选择相应的连接类型。例如，如果您可以从ISP获取由DHCP服务器自动分配的IP地址，请选择“动态IP”；如果您拥有ISP提供的固定IP地址，请选择“静态IP”；如果您的上网的方式为ADSL虚拟拨号方式，请选择“PPPoE”；如果您的上网方式为L2TP的拨号方式，请选择“L2TP”。

上网口令： 请正确输入ISP提供的上网口令，必须填写。

连接/断线： 单击此按钮，可进行即时的连接/断线操作。

动态或静态IP： 如果ISP分配了IP地址、子网掩码、网关和DNS服务器地址，请选择使用静态IP。否则使用动态IP。

服务器IP/域名： 输入由ISP提供的服务器IP或者域名。

IP地址： 当选择使用静态IP时，请输入拨号时使用的IP地址。

子网掩码： 当选择使用静态IP时，请输入ISP提供的子网掩码。

网关： 当选择使用静态IP时，请输入ISP提供的网关IP地址。

DNS： 当选择使用静态IP时，请输入ISP提供的DNS服务器地址。

Internet IP： 从ISP的L2TP服务器得到的因特网IP地址。

Internet DNS： 从ISP的L2TP服务器得到的DNS服务器地址。

数据包MTU： 填入网络数据包的MTU值，缺省为1460，如非特别需要，一般不要更改。

按需连接： 当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若您的网络服务是按时间交费，可以选择该项连接方式。

自动连接： 开机后系统自动连接网络。在使用过程中，如果由于外部原因，网络被断开，系统则会每隔一段时间(30秒)尝试连接，直到成功连接为止。若您的网络服务是包月交费形式，可以选择该项连接方式。

手动连接： 开机或断线后，需要在此处或个人计算机中手动拨号连接。若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若您的网络服务是按时间交费，选择该连接方式可有效节省上网费用。

完成更改后，点击**保存**按钮。

5. PPTP

如果ISP提供的上网方式是PPTP，ISP会给您提供上网帐号和上网口令。具体设置时，若不清楚，请咨询ISP。见图 5-9。

WAN口设置

WAN口连接类型： PPTP

上网帐号： username

上网口令： ●●●●●●●●

连 接 断 线 未连接

动态 IP 静态 IP

服务器 IP /域名：

IP 地址： 0.0.0.0

子网掩码： 0.0.0.0

网关： 0.0.0.0

DNS： 0.0.0.0 , 0.0.0.0

Internet IP： 0.0.0.0

Internet DNS： 0.0.0.0 , 0.0.0.0

数据包MTU(字节)： 1420 （缺省值为1420，如非必要，请勿修改）

根据您的需要，请选择对应的连接模式：

自动断线等待时间： 15 分 （0 表示不自动断线）

按需连接，在有访问数据时自动进行连接

自动连接，在开机和断线后自动连接

手动连接，由用户手动连接

保 存 帮 助

图 5-9 WAN 口设置-PPTP

上网帐号： 请正确输入ISP提供的上网帐号，必须填写。

上网口令： 请正确输入ISP提供的上网口令，必须填写。

连接/断线： 单击此按钮，可进行即时的连接/断线操作。

动态或静态IP： 如果ISP分配了IP地址、子网掩码、网关和DNS服务器地址，请选择使用静态IP。否则使用动态IP。

服务器IP/域名： 输入由ISP提供的服务器IP或者域名。

IP地址： 当选择使用静态IP时，请输入拨号时使用的IP地址。

子网掩码： 当选择使用静态IP时，请输入ISP提供的子网掩码。

网关： 当选择使用静态IP时，请输入ISP提供的网关IP地址。

DNS： 当选择使用静态IP时，请输入ISP提供的DNS服务器地址

Internet IP： 从ISP的PPTP服务器得到的因特网IP地址。

Internet DNS： 从ISP的PPTP服务器得到的DNS服务器地址

数据包MTU： 填入网络数据包的MTU值，缺省为1420，如非特别需要，一般不要更改。

按需连接： 当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若您的网络服务是按时间交费，可以选择该项连接方式。

自动连接： 开机后系统自动连接网络。在使用过程中，如果由于外部原因，网络被断开，系统则会每隔一段时间(30秒)尝试连接，直到成功连接为止。若您的网络服务是包月交费形式，可以选择该项连接方式。

手动连接： 开机或断线后，需要在此处或个人计算机中手动拨号连接。若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若您的网络服务是按时间交费，选择该连接方式可有效节省上网费用。

完成更改后，点击**保存**按钮。

6. DHCP+

如果ISP提供的上网方式是DHCP+，ISP会给您提供上网帐号、上网口令和认证服务器IP地址。具体设置时，若不清楚，请咨询ISP。见图 5-10。

WAN口设置

WAN口连接类型： DHCP+

上网账号： username
上网口令： ••••••••

IP地址： 0.0.0.0
子网掩码： 0.0.0.0
网关： 0.0.0.0
首选DNS服务器： 0.0.0.0
备用DNS服务器： 0.0.0.0

数据包MTU： 1500 （缺省值为1500，如非必要，请勿更改）
认证服务器： 218.29.0.227 （缺省为 218.29.0.227）

根据您的需要，请选择对应连接模式：

自动连接，在开机和断线后自动进行连接。
手动连接，由用户手动进行连接。

连 接 断 线 未连接

保 存 帮 助

图 5-10 WAN 口设置-DHCP+

上网帐号： 请正确输入ISP提供的上网帐号，必须填写。

上网口令： 请正确输入ISP提供的上网口令，必须填写。

数据包MTU： 输入网络数据包的MTU值，缺省为1500，如非特别需要，一般不要更改。

认证服务器： 输入ISP提供的上网认证服务器的地址，若不清楚，可以向ISP咨询。

自动连接： 开机后系统自动连接网络。在使用过程中，如果由于外部原因，网络被断开，则系统会每隔一段时间(10秒)尝试连接，直到成功连接为止。若您的网络服务是包月交费形式，可以选择该项连接方式。

手动连接： 开机或断线后，需要在此处或个人计算机中手动拨号连接。若您的网络服务是按时间交费，选择该连接方式可有效节省上网费用。

连接/断线： 单击相应按钮，可进行即时的连接/断线操作。

完成更改后，点击**保存**按钮。

5.5.2 LAN口设置

在 LAN 口设置中，可以设置路由器的局域网 IP 地址和子网掩码，局域网用户可以通过此 IP 地址管理本路由器。若您为普通的家庭共享上网，则无须改变 LAN 口 IP 地址，保持默认值即可。

选择菜单**网络参数→LAN口设置**，可以在图 5-11界面中配置LAN接口的网络参数。



图 5-11 LAN 口设置

MAC地址： 本路由器对局域网的MAC地址，用来标识局域网。

IP地址： 输入本路由器对局域网的IP地址。局域网中所有计算机的IP地址必须与此IP地址处于同一网段且默认网关必须为此IP地址。该IP地址出厂默认值为192.168.1.1，为C类IP地址，适用于数量不超过200台计算机的小型网络，可以根据组网需要改变它。

子网掩码： 选择路由器对局域网的子网掩码。C类IP地址对应子网掩码为255.255.255.0，为保证网络连接正常，请不要改变子网掩码。可以根据实际的局域网类型以及IP地址类型选择不同的子网掩码。

完成更改后，点击**保存**按钮，路由器将自动重启以使现有设置生效。

☞ 注意：

1. 如果改变了本地IP地址，必须用新的IP地址才能登录路由器的WEB管理界面，并且局域网中所有计算机的默认网关必须设置为该IP地址才能正常上网。

2. 局域网中所有计算机的子网掩码必须与此处子网掩码设置相同。

5.5.3 MAC地址克隆

选择菜单**网络参数→MAC地址克隆**，可以在下图 5-12界面中设置路由器对广域网的MAC地址。

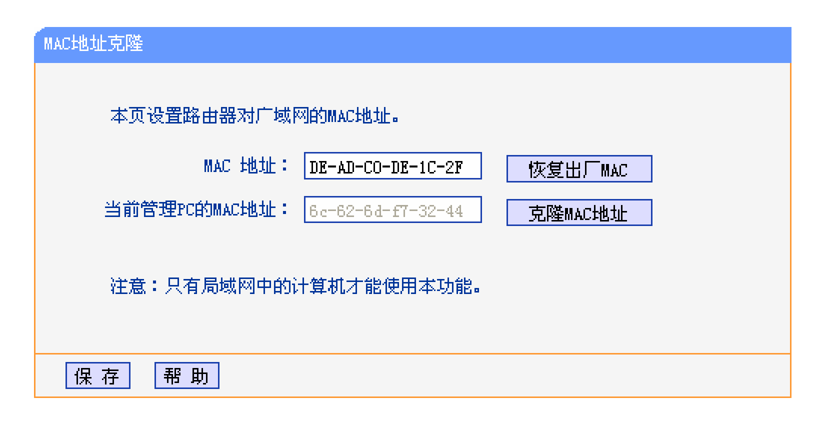


图 5-12 MAC 地址克隆

MAC地址： 此项默认为路由器WAN口的MAC地址。若ISP提供了一个MAC地址给您并要求对路由器WAN口的MAC地址进行绑定，则只要将提供的值输入到"MAC地址"栏即可。除非ISP有特别要求，否则不建议更改MAC地址。

当前管理PC的MAC地址：

该处显示当前正在管理路由器的计算机的MAC地址。

恢复出厂MAC： 单击此按钮，即可恢复MAC地址为出厂时的默认值。

克隆MAC地址： 单击此按钮，可将当前管理PC的MAC地址克隆到"MAC地址"栏内。若ISP提供服务时要求进行MAC地址克隆，则应进行该项操作，否则无须克隆MAC地址。

完成更改后，点击**保存**按钮。

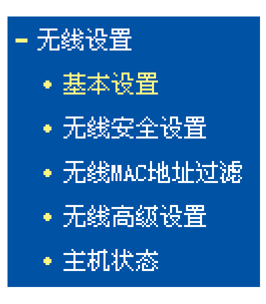
☞ 注意：

只有局域网中的计算机才能使用"MAC地址克隆"功能。

5.6 无线设置

通过无线设置功能，可以安全方便的启用路由器的无线功能进行网络连接。

选择菜单**无线设置**，可以看到：



单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.6.1 基本设置

通过进行基本设置可以开启并使用路由器的无线功能，组建内部无线网络。（组建网络时，内网主机需要无线网卡来连接到无线网络）但是此时的无线网络并不是安全的，建议您完成基本设置后进行相应的无线安全设置。

单击**基本设置**，可以在图 5-13中进行无线网络的基本设置。其中的SSID号和信道是路由器无线功能必须设置的参数。



图 5-13 无线网络基本设置

SSID： 即 Service Set Identification，用于标识无线网络的网络名称。可以在此输入一个您喜欢的名称，它将显示在无线网卡搜索到的无线网络列表中。

频段： 决定无线信号工作的频率带宽，可选项有 2.4GHz 和 5GHz。

模式： 该项用于设置路由器的无线工作模式。频段选为 2.4GHz 时，推荐使用 11bgn mixed 模式；频段选为 5GHz 时，推荐使用 11an mixed 模式。

频段带宽： 设置无线数据传输时所占用的信道宽度，可选项有 20M、40M 和自动。

信道： 以无线信号作为传输媒体的数据信号传送的通道，若选自动，则 AP 会自动根据周围的环境选择一个最好的信道。若频段选为 2.4GHz，信道可选择 1~13；若频段选为 5GHz，信道可选择 149、153、157、161 或 165。

最大发送速率： 该项用于设置无线网络的最大发送速率。

开启无线功能： 若要采用路由器的无线功能，必须选择该项，这样，无线网络内的主机才可以接入并访问有线网络。

开启 SSID 广播： 该项功能用于将路由器的 SSID 号向周围环境的无线网络内广播，这样，主机才能扫描到 SSID 号，并可以加入该 SSID 标识的无线网络。

开启 WDS： 可以选择这一项开启 WDS 功能，通过这个功能可以桥接多个无线局域网。

完成更改后，点击**保存**按钮并重启路由器使现在的设置生效。

☞ 注意：

1. 选择信道时请避免与当前环境中其他无线网络所使用的信道重复，以免发生信道冲突，使传输速率降低。
2. 以上提到的频段带宽设置仅针对支持IEEE 802.11n协议的网络设备；对于不支持IEEE 802.11n协议的设备，此设置不生效。例如，当本路由器与11N系列网卡客户端进行通信时频道带宽设置可以生效，当与11a/b/g系列网卡客户端进行通信时此设置将不再生效。
3. 路由器默认无线工作于2.4GHz频段，若需调至5GHz频段，请登录路由器设置界面进行如下操作：无线设置→基本设置→频段（选为5GHz）→保存，重启路由器生效。
4. 若您的终端设备不支持5GHz频段，而路由器的频段设置为5GHz，则该终端设备将无法搜索到路由器的无线信号。
5. 当路由器的无线设置完成后，无线网络内的主机若想连接该路由器，其无线参数（如SSID号）必须与此处设置一致。
6. 与路由器进行WDS连接的AP，只需要工作在AP模式且支持4地址即可，不需要额外的配置。WDS的连接拓扑图如图5-14。

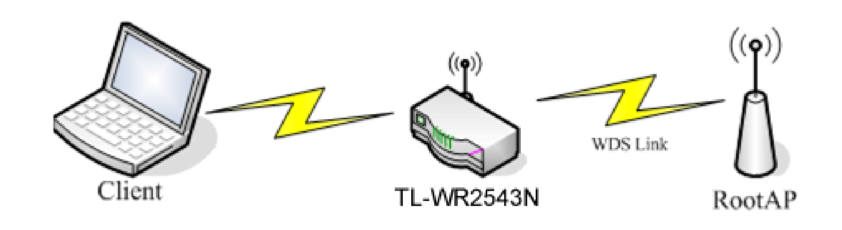


图 5-14 WDS 连接拓扑图

5.6.2 无线安全设置

通过无线安全设置功能，可以防止他人未经同意私自连入您的无线网络，占用网络资源，同时也可以避免黑客窃听、黑客攻击等不利行为，从而提高无线网络的安全性。

选择菜单**无线设置→无线安全设置**，可以在图 5-15界面中设置无线网络安全选项。

无线网络安全设置

本页面设置路由器无线网络的安全认证选项。
安全提示：为保障网络安全，强烈推荐开启安全设置，并使用WPA-PSK/WPA2-PSK AES加密方法。

不开启无线安全

WPA-PSK/WPA2-PSK

认证类型：自动
加密算法：AES
PSK密码：
（8-63个ASCII码字符或8-64个十六进制字符）
组密钥更新周期：86400 （单位为秒，最小值为30，不更新则为0）

WPA/WPA2

认证类型：自动
加密算法：自动
Radius服务器IP：
Radius端口：1812 （1-65535，0表示默认端口：1812）
Radius密码：
组密钥更新周期：0 （单位为秒，最小值为30，不更新则为0）

WEP

认证类型：自动
WEP密钥格式：十六进制

密钥选择	WEP密钥	密钥类型
密钥 1：		禁用
密钥 2：		禁用
密钥 3：		禁用
密钥 4：		禁用

保存 帮 助

图 5-15 无线网络安全设置

在无线网络安全设置页面，可以选择是否开启无线安全功能。

- 如果无需开启无线安全功能，请勾选**不开启无线安全**。
- 如果需要开启无线安全功能，则请选择页面中三种安全类型中的一种进行无线安全设置。为保障网络安全，强烈推荐您开启安全设置，并使用WPA-PSK/WPA2-PSK加密方法。

本页面提供了三种无线安全类型：WPA-PSK/WPA2-PSK、WPA/WPA2 以及 WEP。不同的安全类型下，安全设置项不同，下面将详细介绍。

1. WPA-PSK/WPA2-PSK

WPA-PSK/WPA2-PSK安全类型是基于共享密钥的WPA模式，安全性很高，设置也比较简单，适合普通家庭用户和小型企业使用。其具体设置项见下图5-16示。

WPA-PSK/WPA2-PSK
认证类型： 自动
加密算法： AES
PSK密码：
（8-63个ASCII码字符或8-64个十六进制字符）
组密钥更新周期： 86400 （单位为秒，最小值为30，不更新则为0）

图 5-16 WPA-PSK/WPA2-PSK 安全模式

认证类型： 该项用来选择系统采用的安全模式，即自动、WPA-PSK、WPA2-PSK。

- 自动：若选择该项，路由器会根据主机请求自动选择WPA-PSK或WPA2-PSK安全模式。
- WPA-PSK：若选择该项，路由器将采用WPA-PSK的安全模式。
- WPA2-PSK：若选择该项，路由器将采用WPA2-PSK的安全模式。

加密算法： 该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。默认选项为自动，选择该项后，路由器将根据实际需要自动选择TKIP或AES加密方式。注意11N模式不支持TKIP算法。

PSK密码： 该项是WPA-PSK/WPA2-PSK的初始设置密钥，设置时，要求为8-63个ASCII字符或8-64个十六进制字符。

组密钥更新周期： 该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为30，若该值为0，则表示不进行更新。

2. WPA/WPA2

WPA/WPA2是采用Radius服务器进行身份认证并得到密钥的WPA或WPA2安全模式。由于要架设一台专用的认证服务器，代价比较昂贵且维护也很复杂，所以不推荐普通用户使用此安全类型。其具体设置项见下图5-17示。

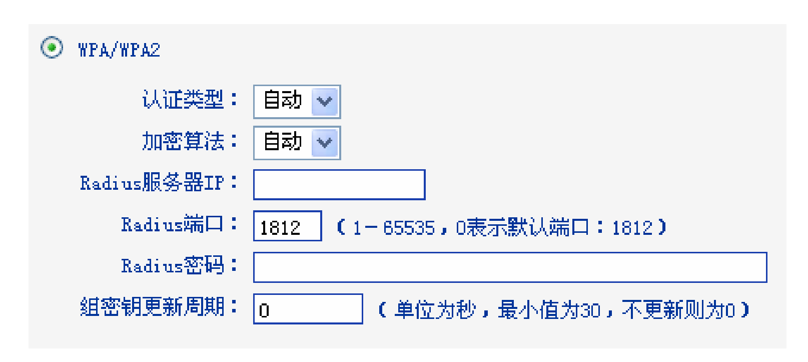


图 5-17 WPA/WPA2 安全模式

认证类型： 该项用来选择系统采用的安全模式，即自动、WPA、WPA2。

- 自动：若选择该项，路由器会根据主机请求自动选择WPA或WPA2安全模式。
- WPA：若选择该项，路由器将采用WPA的安全模式。

- WPA2：若选择该项，路由器将采用WPA2的安全模式。

加密算法： 该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。默认选项为自动，选择该项后，路由器将根据实际需要自动选择TKIP或AES加密方式。这里需要注意的是，选择WPA/WPA2 TKIP加密时，由于802.11N不支持此加密方式，所以路由器可能工作在较低的传输速率上，建议使用WPA2-PSK等级的AES加密。如图5-18。

WPA/WPA2
认证类型：自动
加密算法：TKIP
Radius服务器IP：
Radius端口：1812 （1－65535，0表示默认端口：1812）
Radius密码：
组密钥更新周期：0 （单位为秒，最小值为30，不更新则为0）
注意：您选择的TKIP加密算法经常在老的无线网卡上使用，新的802.11n不支持此加密算法。所以，如果您选择了此加密算法，路由器可能工作在较低的传输速率上。建议使用AES加密算法。

图 5-18 选择 WPA/WPA2 TKIP 加密

Radius服务器IP： Radius服务器用来对无线网络内的主机进行身份认证，此项用来设置该服务器的IP地址。

Radius端口： Radius服务器用来对无线网络内的主机进行身份认证，此项用来设置该Radius认证服务采用的端口号。

Radius密码： 该项用来设置访问Radius服务的密码。

组密钥更新周期： 该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为30，若该值为0，则表示不进行更新。

3. WEP

WEP是Wired Equivalent Privacy的缩写，它是一种基本的加密方法，其安全性不如另外两种安全类型高。选择WEP安全类型，路由器将使用802.11基本的WEP安全模式。这里需要注意的是因为802.11N不支持此加密方式，若选择此加密方式，路由器可能会工作在较低的传输速率上。其具体设置项见下图5-19示。

WEP

认证类型：自动

WEP密钥格式：十六进制

密钥选择		WEP密钥	密钥类型
密钥 1：	◉		禁用
密钥 2：	○		禁用
密钥 3：	○		禁用
密钥 4：	○		禁用

注意：您选择的WEP加密经常在老的无线网卡上使用，新的802.11n不支持此加密方式。所以，如果您选择了此加密方式，路由器可能工作在较低的传输速率上。建议使用WPA2-PSK等级的AES加密。

图 5-19 WEP 安全模式

认证类型： 该项用来选择系统采用的安全模式，包括自动、开放系统、共享密钥。

- 自动：若选择该项，路由器会根据主机请求自动选择开放系统或共享密钥方式。
- 开放系统：若选择该项，路由器将采用开放系统方式。此时，无线网络内的主机可以在不提供认证密码的前提下，通过认证并关联上无线网络，但是若要进行数据传输，必须提供正确的密码。
- 共享密钥：若选择该项，路由器将采用共享密钥方式。此时，无线网络内的主机必须提供正确的密码才能通过认证，否则无法关联上无线网络，更无法进行数据传输。

WEP密钥格式： 该项用来选择即将设置的密钥的形式，包括16进制、ASCII码。若采用16进制，则密钥字符只能为0～9，A、B、C、D、E、F；若采用ASCII码，则密钥字符可以是键盘上的任意字符。

密钥选择、WEP密钥、密钥类型：

这三项用来选择密钥，设置具体的密钥值和选择密钥的类型，密钥的长度受密钥类型的影响。

密钥长度说明：选择64位密钥需输入16进制字符10个，或者ASCII码字符5个。选择128位密钥需输入16进制字符26个，或者ASCII码字符13个。选择152位密钥需输入16进制字符32个，或者ASCII码字符16个。

密钥选择中的4个密钥，可以只使用其一，也可以多个同时使用。无论哪种情况，客户端网卡上密钥的设置都必须与之一一对应。

☞ 注意：

若路由器进行了无线安全设置，则该无线网络内的所有主机都必须根据此处的安全设置进行相应的设置，如密码设置必须完全一样，否则将不能成功的通过无线连接到该路由器。

5.6.3 无线MAC地址过滤

MAC 地址是网卡的物理地址，它就像是网卡的身份证，在网络中进行网卡的识别都是通过这个地址进行的。通常说的计算机的 MAC 地址也即计算机上网卡的 MAC 地址。

无线 MAC 地址过滤功能就是通过 MAC 地址来控制计算机能否接入无线网络，从而有效控制无线网络内用户的上网权限。

无线 MAC 地址过滤功能通过 MAC 地址允许或拒绝无线网络中的计算机访问广域网，有效控制无线网络内用户的上网权限。可以点击按钮**添加新条目**来增加新的过滤规则；或者通过“编辑”、“删除”链接来编辑或删除列表中的过滤规则。



图 5-20 无线网络 MAC 地址过滤设置

MAC地址过滤功能：

请在该处选择是否开启路由器的无线网络MAC地址过滤功能。只有选择开启时，下面的设置才会生效。

过滤规则： 请选择MAC地址过滤规则，允许或禁止列表中生效规则之外的MAC地址所对应的计算机访问本无线网络。

点击**添加新条目**按钮后，可以在图5-21界面中设置过滤规则条目：

无线网络MAC地址过滤设置

本页设置MAC地址过滤来控制计算机对本无线网络的访问。

MAC 地址：

描述：

状态： 生效

保 存 返 回 帮 助

图 5-21 无线网络 MAC 地址过滤设置

MAC地址： 用于输入被管理的计算机的MAC地址。

状态： 用于设置MAC地址过滤条目的状态。“生效”表示该设置条目被启用，“失效”表示该设置条目未被启用。

描述： 对主机的简单描述，可选设置，但为了便于识别不同的计算机，建议进行设置。

设置完成后，设置结果将显示在图5-20中列表当中。

举例：如果您想禁止MAC地址为“00-13-8F-A9-E6-CA”和“00-13-8F-A9-E6-CB”的主机访问您的无线网络，而其他主机可以访问此无线网络，请按照以下步骤进行配置：

1. 在图 5-20中，选择过滤规则为“允许列表中生效规则之外的MAC地址访问本无线网络”，并确认访问控制列表中没有任何你不需要过滤的MAC地址生效条目，如果有，将该条目状态改为“失效”或删除该条目，也可以点击**删除所有条目**按钮，将列表中的条目清空。
2. 在图 5-20中，点击**添加新条目**按钮，按照下图 5-22界面，设置MAC地址为“00-13-8F-A9-E6-CA”，状态为“生效”。设置完成后，点击**保存**按钮。

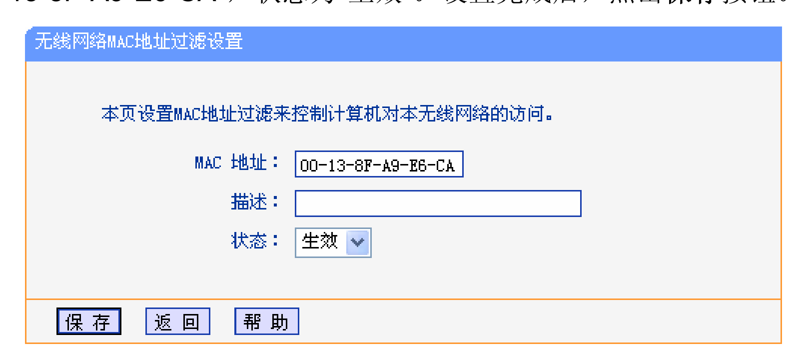


图 5-22 添加无线网络 MAC 地址过滤条目

3. 参照第三步，继续添加过滤条目，设置 MAC 地址为“00-13-8F-A9-E6-CB”，状态为“生效”。设置完成后，点击**保存**按钮。
4. 在图 5-20中，点击**启用过滤**按钮，开启无线网络的访问控制功能。

例1中设置完成后生成的MAC地址过滤列表为：

ID	MAC地址	状态	描 述	编 辑
1	00-13-8F-A9-E6-CA	生效		编辑 删除
2	00-13-8F-A9-E6-CB	生效		编辑 删除

☞ 注意：

如果您开启了无线网络的MAC地址过滤功能，并且过滤规则选择了“禁止列表中生效规则之外的MAC地址访问本无线网络”，而过滤列表中又没有任何生效的条目，那么任何主机都不可以访问本无线网络。

5.6.4 无线高级设置

此界面用于设置路由器的高级无线功能，建议这些操作由专业人员进行，因为不正确的设置可能会降低路由器的无线性能。

选择菜单**无线设置→无线高级设置**，可以看到如下图 5-23的无线高级设置界面。



图 5-23 无线高级设置

传输功率： 设置无线网络的传输功率，推荐保持默认值“高”。

Beacon时槽： 路由器通过发送Beacon广播进行无线网络连接的同步。Beacon时槽表示路由器发送Beacon广播的频率。默认值为100毫秒。Beacon广播的取值范围是40－1000毫秒。

RTS时槽： 为数据包指定RTS（Request to Send，发送请求）阈值。当数据包长度超过RTS阈值时，路由器就会发送RTS到目的站点来进行协商。接收到RTS帧后，无线站点会回应一个CTS（Clear to Send，清除发送）帧来回应路由器，表示两者之间可以进行无线通信了。

分片阈值： 为数据包指定分片阈值。当数据包的长度超过分片阈值时，会被自动分成多个数据包。过多的数据包将会导致网络性能降低，所以分片阈值不应设置过低。默认值为2346。

DTIM阈值： 该值在1至15 毫秒之间，指定传输指示消息(DTIM)的间隔。DTIM是一种倒数计时作业，用以告知下一个要接收广播及多播的客户端窗口。当路由器已经为相关联的客户端缓存了广播或者多播信息时，它会在Beacon中夹带有下一个DTIM时槽的信息；当客户端听到Beacon讯号时，就会接收该广播和组播信息。默认值为1。

开启WMM： 开启WMM后路由器具有无线服务质量功能，可以对音频、视频数据优先处理，保证音频、视频数据的优先传输。推荐您勾选此项。

开启Short GI： 选择此项可以使路由器接收和发送短帧间隔数据包，提高路由器的传输速率，推荐勾选。

开启AP隔离： 选择此项可以隔离关联到AP的各个无线站点。

完成更改后，点击保存按钮。

5.6.5 主机状态

此页面显示连接到本无线网络中的所有主机的基本信息。选择菜单**无线设置→主机状态**，可以在下图 5-24界面中查看当前连接到无线网络中的所有主机的基本信息。单击**刷新**按钮，可以更新列表中的条目信息。



图 5-24 无线网络主机状态

MAC地址： 显示当前已经连接到无线网络的主机的MAC地址。

当前状态： 显示当前主机的运行状态。

接收数据包数、发送数据包数：

显示当前主机接收和发送的数据包的总数。

5.7 DHCP服务器

DHCP，即 Dynamic Host Control Protocol，动态主机控制协议。TL-WR2543N 有一个内置的 DHCP 服务器，可以实现局域网内的计算机 IP 地址的自动分配。

选择菜单 **DHCP 服务器**，可以看到：



单击菜单中的某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.7.1 DHCP服务

如果启用了DHCP服务功能，并将计算机获取IP的方式设为“自动获得IP地址”，则当您打开计算机时，DHCP服务器会自动从地址池中分配未被使用的IP地址到您的计算机，而不需要手动进行设置。

选择菜单**DHCP服务器→DHCP服务**，可以看到DHCP设置界面，如图 5-25。

DHCP服务

本路由器内建的DHCP服务器能自动配置局域网中各计算机的TCP/IP协议。

DHCP服务器： 不启用 启用

地址池开始地址： 192.168.1.100

地址池结束地址： 192.168.1.199

地址租期： 120 分钟 （1～2880分钟，缺省为120分钟）

网关： 192.168.1.1 （可选）

缺省域名： （可选）

主DNS服务器： 0.0.0.0 （可选）

备用DNS服务器： 0.0.0.0 （可选）

保 存 帮 助

图 5-25 DHCP 服务

DHCP服务器： 选择是否启用DHCP服务器功能，默认为启用。

地址池开始/结束地址： 分别输入开始地址和结束地址。完成设置后，DHCP服务器分配给内网主机的IP地址将介于这两个地址之间。

地址租期： 即DHCP服务器给内网主机分配的IP地址的有效使用时间。在该段时间内，服务器不会将该IP地址分配给其它主机。

网关： 可选项。应填入路由器LAN口的IP地址，缺省为192.168.1.1。

缺省域名： 可选项。应填入本地网域名，缺省为空。

主/备用DNS服务器： 可选项。可以填入ISP提供的DNS服务器或保持缺省，若不清楚可咨询您的ISP。

完成更改后，点击**保存**按钮并重启路由器使设置生效。

☞ 注意：

若要使用本路由器的 DHCP 服务器功能：

1. 局域网中计算机获取 IP 的方式必须设置为“自动获得 IP 地址”,设置方法详见附录 X;
2. 必须事先指定 IP 地址池的开始和结束地址。

5.7.2 客户端列表

客户端列表显示当前所有通过 DHCP 服务器获得 IP 地址的客户端主机的相关信息，包括客户端名、MAC 地址、所获得的 IP 地址、及 IP 地址的有效时间。

选择菜单**DHCP服务器→客户端列表**，可以查看客户端主机的相关信息；单击**刷新**按钮可以更新表中信息，如图 5-26。

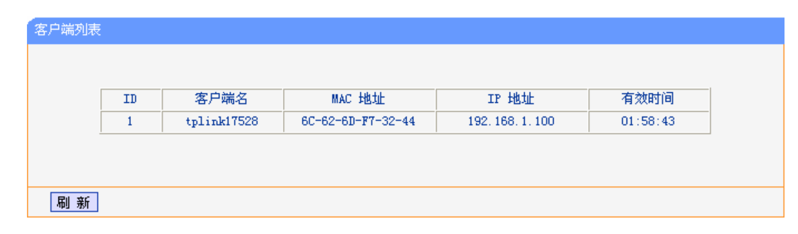


图 5-26 客户端列表

客户端名： 显示获得IP地址的客户端计算机的名称。

MAC地址： 显示获得IP地址的客户端计算机的MAC地址。

IP地址： 显示DHCP服务器分配给客户端主机的IP地址。

有效时间： 指客户端主机获得的IP地址距到期所剩的时间。每个IP地址都有一定的租用时间，客户端软件会在租期到期前自动续约。

5.7.3 静态地址分配

静态地址分配功能可以为指定MAC地址的计算机预留IP地址。当该计算机请求DHCP服务器分配IP地址时，DHCP服务器将给它分配表中预留的IP地址。

选择菜单**DHCP服务器→静态地址分配**，可以在下图 5-27所示界面中查看和编辑静态IP地址分配条目。



图 5-27 静态地址分配

点击**添加新条目**按钮，可以在图 5-28所示界面中设置新的静态地址分配条目。

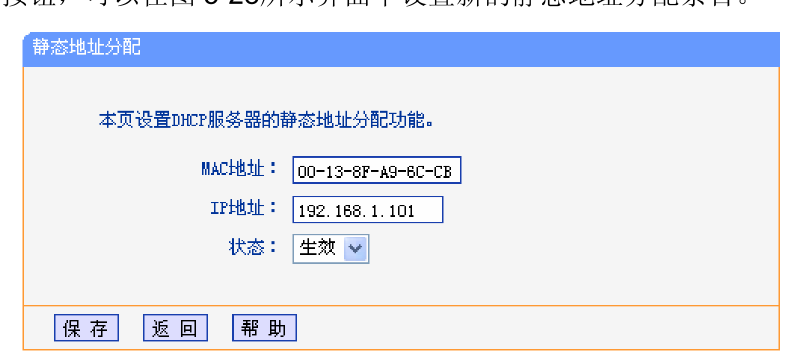


图 5-28 添加静态地址条目

MAC地址： 输入需要预留静态IP地址的计算机的MAC地址。

IP地址： 预留给内网主机的IP地址。

状态： 设置该条目是否生效。只有状态为生效时，本条目的设置才生效。

举例：如果您希望给局域网中MAC地址为00-13-8F-A9-6C-CB的计算机预留IP地址192.168.1.101。请按照如下步骤设置：

1. 在图5-27界面中单击**添加新条目**按钮。
2. 在图5-28界面中设置MAC地址为“00-13-8F-A9-6C-CB”，IP地址为“192.168.1.101”，状态为“生效”。
3. 点击**保存**按钮，可以看到设置完成后的静态地址分配列表如图 5-27所示。
4. 重启路由器使设置生效。

5.8 网络共享

通过使用网络共享服务，可以方便地在局域网中共享 USB 存储设备上的卷。

选择菜单**网络共享**，可以看到：



单击菜单中的子项即可进行具体的设置，下面将详细讲解各子项的功能和设置方法。

5.8.1 网络共享管理

通过网络共享管理功能，可以查看已连接到路由器 USB 口的 USB 存储设备的信息，方便地在局域网中共享 USB 存储设备上的卷。

选择菜单**网络共享→网络共享管理**，可以在图 5-29所示界面中查看网络共享服务条目。



图 5-29 网络共享管理

设备状态： 指示是否启用网络共享服务。

使用密码访问：

如果勾选，局域网中用户必须通过用户名和密码来访问 USB 存储设备上的卷。如果您没有设置访问密码，请启动服务前在“共享账户”页面进行设置。

卷： USB 存储设备上卷的卷名，由路由器自定义，不可更改。

总容量： 显示该卷的大小。

已使用： 显示该卷已被使用的空间大小。

剩余： 显示该卷尚未使用的空间大小。

使用量： 显示该卷已被使用的空间占总空间的百分比。

共享控制： 通过点击该条目下方对应的按钮设置是否共享该卷。点击“启用”，则该卷被共享。

查看： 如果当前卷已启用共享，点击“打开磁盘”，或者在 IE 浏览器中输入“\\路由器 LAN 口 IP 地址\共享名”（如：\\192.168.1.1\volume1），可以查看卷中文件。

弹出设备： 点击该按钮可以安全地移除连接中的 USB 驱动器。

重新扫描： 点击该按钮重新检测 USB 存储设备的信息和共享卷的信息。

☞ 注意：

1. 在拔出USB存储设备前，请先点击图5-29界面上的**弹出设备**按钮，待“可以移除”的提示出现后方可拔出，否则可能造成USB存储设备的损坏或数据丢失。
2. 本路由器支持最多8个分区，8个卷之后的卷将不被显示。
3. 因NTFS支持大文件和大分区，故推荐使用NTFS作为共享卷的文件系统。

举例：假如您希望共享 USB 存储设备上的卷，请按照如下步骤进行设置：

1. 将您的 USB 存储设备（如移动硬盘、U 盘等）插入路由器的 USB 口，等待约 6～10 秒后点击“重新扫描”按钮检测分区信息。
2. 待分区信息显示在列表中后，选择您需要共享的卷，点击“共享控制”栏的“启用”按钮。
3. 点击“设备状态”的“启动”按钮启动网络共享服务。

上述步骤完成之后，您就可以点击“打开磁盘”或在IE浏览器中输入“\\路由器LAN口IP地址\共享名”（如：\\192.168.1.1\volume1）来访问该共享卷了。如果您不清楚路由器当前的IP地址，可以到“运行状态”页中查看。

5.8.2 FTP服务器

选择菜单**网络共享→FTP服务器**，可以在图 5-30所示界面方便地建立起属于您自己的FTP服务器。

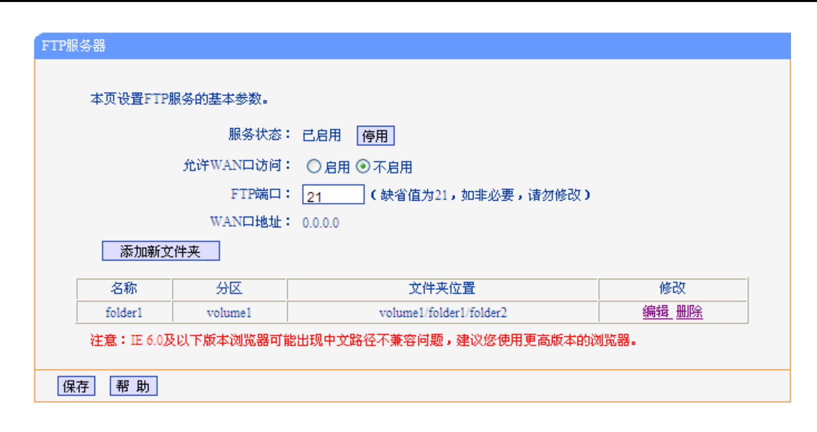


图 5-30 FTP 服务器

服务状态：　设置是否启动 FTP 服务器。

允许 WAN 口访问：　控制 FTP 服务器是否允许从 WAN 口访问。在页面上，您可以看到"WAN 口地址"，如果您使用的是 PPPOE/L2TP/PPTP 拨号方式并且允许从 WAN 口访问， 那么可以通过两种方式访问服务器：同一局域网的用户可以通过"公共地址"来访问；Internet 的用户则可以通过"WAN 口地址"访问。

FTP 端口：　指定 FTP 服务器端口。建议设置为默认值 21。

WAN 口地址：　显示路由器的 WAN 口 IP 地址。

公共地址：　从 ISP 的服务器得到的因特网 IP 地址，即 Internet IP。只有当您使用的是 PPPOE/L2TP/PPTP 拨号上网时，该地址才会显示并有效。

添加新文件夹：　单击该按钮在FTP服务器上新增一个文件夹，并可在图 5-31对其进行设置。

名称：　FTP 服务器上共享文件夹显示的名称。

分区：　该文件夹所在 USB 存储设备的卷标。

文件夹位置：　显示该文件夹的物理完整路径。

修改：　单击该项下的“编辑”或“删除”按钮来编辑或删除指定的共享文件夹。

举例：假如您希望使用 FTP 服务器功能，请按照如下步骤进行设置：

1. 将您的 USB 存储设备（如移动硬盘、U 盘等）插入路由器的 USB 口。
2. 待服务状态显示为"已启用"，您可以设置您的 FTP 服务器的端口，是否启用允许 WAN 口访问等配置项。
3. 点击"保存"。如果您修改了 FTP 服务器的设置，新的设置需重新启动 FTP 服务器才能生效，即先点击"停用"按钮，再点击"启用"按钮。
4. 如果您的FTP服务器上还没有文件夹，您可以点击"添加新文件夹"按钮前往图 5-31所示"新增或修改FTP服务器文件夹"页面进行设置。

上述步骤完成之后，您就可以按“Windows + R”组合键，在打开的“运行”对话框的输入栏或在 IE 浏览器的地址栏输入“ftp:\\路由器 LAN 口 IP 地址:端口”（如：ftp:\\192.168.1.1:21）来访问 FTP 服务器了。如果您不清楚路由器当前的 IP 地址，可以到“运行状态”页中查看。

☞ 注意：

1. FTP服务器最多有10个共享文件夹。当您的FTP服务器共享文件夹达到10个的时候，如果您想共享一个新的文件夹，那么您必须删除一个已有的文件夹后再添加。
2. 访问FTP服务器需要具有FTP访问权限的账户才能正常访问。如果您需要修改您的访问权限或账户，请启动服务前在“共享帐户”页设置。

单击“添加新文件夹”或“修改”项中的“编辑”按钮，出现以下界面，在该界面中可对新增或要修改的共享文件夹进行设置，如图 5-31所示。



图 5-31 新增或修改共享文件夹

名称： 指定 FTP 服务器上共享文件夹显示的名称。

文件夹： 如果勾选“选择全部”，则该文件夹下的所有文件将被共享。

文件夹位置： 显示文件夹所在的完整路径。

返回上一级目录： 显示当前文件夹上一级的父文件夹。

举例：假如您希望在 FTP 服务器上共享 USB 存储设备上 folder1 文件夹下的 folder2 文件夹中的图片（假设已存在），并命名为“我的共享 2”，那么您可以进行如下设置：

1. 在文件夹列表下找到 folder1 文件夹。
2. 点击“folder1”的链接，展开 folder1 目录下的文件夹情况。
3. 在 folder1 文件夹列表下，找到 folder2 文件夹，点选该文件夹的“选择”按钮。如果 folder1 目录下只有 folder2 文件夹，那么您可以选择“文件夹”的“选择全部”。
4. 在“名称”栏输入“我的共享 2”。
5. 点击保存。

以上设置完成后，在返回的“媒体服务器”页面可以看到如下信息：

名称	分区	文件夹位置	修改
我的共享	volume1	volume1	编辑 删除
我的共享2	volume1	volume1/folder1/folder2	编辑 删除

5.8.3 媒体服务器

选择菜单**网络共享→媒体服务器**，可以在图 5-32所示界面方便地建立起属于您自己的媒体服务器。



图 5-32 媒体服务器

服务器名称： 媒体播放器中显示的服务器名称。

服务器状态： 设置是否启动媒体服务器。如果已停用，可点击“启用”按钮启动服务器。

自动扫描： 勾选该项则可通过设置时间间隔让服务器自动扫描共享文件夹。

全部扫描： 扫描媒体服务器上所有共享文件夹下的媒体文件。

新增文件夹： 可以添加媒体服务器扫描的共享文件夹。如果您的媒体服务器上还没有共享文件夹，点击“新增文件夹”按钮前往图 5-33所示“添加媒体服务器文件夹”页面进行设置。

名称： 标识服务器上共享文件夹的名称。

文件系统： 共享文件夹的文件系统。本路由器支持 FAT32 和 NTFS 文件系统。

文件夹： 显示文件夹所在完整路径。

删除： 点击“删除”按钮删除指定的文件夹。

☞ 注意：

媒体服务器最多有6个共享文件夹。当您的服务器共享文件夹达到6个的时候， 如果您想共享一个新的文件夹，那么您必须删除一个已有的文件夹后再添加。

单击“新增文件夹”按钮，出现以下界面，在该界面中可对新增或要修改的共享文件夹进行设置，如图 5-33所示。



图 5-33 新增媒体服务器文件夹

名称：　　　　　　　指定 FTP 服务器上共享文件夹显示的名称。

文件夹：　　　　　　如果勾选“选择全部”，则该文件夹下的所有文件将被共享。

文件夹位置：　　　　显示文件夹所在的完整路径。

返回上一级目录：　　显示当前文件夹的父文件夹目录。

举例：假如您希望您的媒体播放器能够浏览 USB 存储设备上 folder1 文件夹下的 folder2 文件夹中的图片（假设已存在），并命名为“我的媒体”，那么您可以进行如下设置：

1. 在文件夹列表下找到 folder1 文件夹。
2. 点击“folder1”的链接，展开 folder1 目录下的文件夹情况。
3. 在 folder1 文件夹列表下，找到 folder2 文件夹，点选该文件夹的“选择”按钮。如果 folder1 目录下只有 folder2 文件夹，那么您可以选择“文件夹”的“选择全部”。
4. 在“名称”栏输入“我的媒体”。
5. 点击保存。

以上设置完成后，在返回的“媒体服务器”页面可以看到如下信息：

名称	文件系统	文件夹	删除
我的媒体	FAT32	/folder1/folder2	删除

5.8.4　共享帐户

选择菜单**网络共享→共享帐户**，可以在图 5-34所示界面中设置网络共享用户的用户名和密码。



图 5-34 共享帐户

在启用共享之前，请先给共享帐户设置用户名和密码。

两个默认共享帐户分别是超级用户“admin”和普通用户“guest”。超级用户对可写的共享卷具有读/写权限，对只读的共享卷具有只读权限，而普通用户在任何情况下都只具有只读权限，无论该卷的读写权限是只读还是可写，并且仅超级用户能够通过 IE 浏览器上传文件到可写的共享卷中。

您可以通过点击新增使用者按钮增添使用者账户，如图 5-35所示。

每个帐户均需要指定使用者账号及密码。

添加或修改共享账户

本页可以添加或修改服务器的管理者和使用者的账户。

使用者账号： admin2

密码： •••••

确认密码： •••••

存取权限： 只读

FTP访问： 否

保存 返回

图 5-35 新增使用者

使用者账号：由不超过 15 个字符的英文字母、数字、下划线组成。超级用户和普通用户的账号名不能相同。

密码： 由不超过 15 个字符的英文字母、数字、下划线组成。

确认密码： 输入的确认密码必须和上面的密码一致。

存取权限： 通过设置存取权限区分超级用户和普通用户。可选权限为读写或只读。

FTP 访问： 设置该账户对 FTP 服务器的使用权限。

完成设置后，点击**保存**按钮并重启服务使新设置生效。

注意：

1. 如果您更改了共享账户设置后无法使用新设置的用户名和密码访问共享卷，请尝试按“Windows + R”组合键，在打开的“运行”对话框的输入栏中输入“net use \\192.168.1.1 /delete /yes ”后回车。此处 192.168.1.1 是您路由器当前的LAN口IP地址。如果您不清楚路由器当前的IP地址，可以到状态页中查看。
2. 更改帐户设置后，请重启服务使新设置生效。

5.9 转发规则

通过转发规则功能，可以使远程用户访问您局域网计算机上的资源，还可以在局域网用户运行某些特殊应用程序（如 Internet 网络游戏、视频会议、网络电话）时，建立用户端与因特网服务器之间的连接。

选择菜单**转发规则**，可以看到：



单击菜单中的子项即可进行具体的设置，下面将详细讲解各子项的功能和设置方法。

5.9.1 虚拟服务器

通过将本路由器配置为虚拟服务器，可以使远程用户访问局域网内部的服务器，如 Web、FTP、邮件服务器等。

为保证局域网的安全，默认情况下，路由器会将局域网主机的 IP 地址隐藏起来，使因特网计算机无法主动与局域网计算机建立连接。因此，若要使因特网用户能够访问局域网内的服务器，需要设置虚拟服务器条目。

“虚拟服务器”定义了路由器的因特网服务端口与局域网服务器 IP 地址之间的对应关系。因特网所有对此端口的服务请求都会转发给通过 IP 地址指定的局域网服务器，这样既保证了因特网用户成功访问局域网中的服务器，又不影响局域网内部的网络安全。

选择菜单**转发规则→虚拟服务器**，可以在图 5-36所示界面中查看和编辑虚拟服务器条目。



图 5-36 虚拟服务器

点击**添加新条目**按钮，可以在图 5-37所示界面中设置新的虚拟服务器条目。

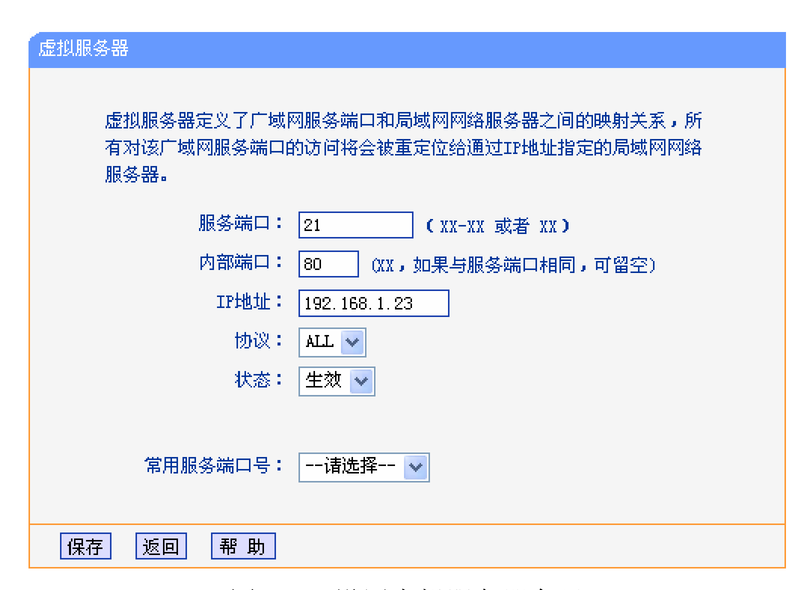


图 5-37 设置虚拟服务器条目

服务端口： 设置路由器向因特网开放的服务端口。因特网用户通过向该端口发送请求来获取服务。可输入单个端口值或连续的端口段。端口段输入格式为“开始端口-结束端口”。

内部端口： LAN 端服务端口，即路由器提供给局域网的服务端口。如果内部端口与服务端口相同，您可以留空，或者输入一个具体端口号。

IP 地址： 输入局域网服务器的静态 IP 地址。通过此 IP 地址，路由器会将对服务端口的访问请求转到局域网服务器上。

协议： 选择此虚拟服务所采用的协议，可选项有 TCP、UDP 和 ALL。若对采用的协议不清楚，推荐选择 ALL。

状态： 设置该条目是否生效。只有状态为生效时，本条目的设置才有效。

常用服务端口号： 选择服务器提供的服务类型，系统会自动将该服务的服务端口号和协议添加到上述对应项中。对于“常用服务端口号”中没有列出的服务，需要手动输入服务端口号和协议的相关信息。

举例： 假如您有一些大型文件要共享给局域网以外的朋友，而由于文件太大，传输起来不方便，这时可以将自己的计算机构建成 FTP 服务器，然后利用本路由器的虚拟服务器功能使您的朋友可以访问您计算机中的这些文件。假设 FTP 服务器（即您的计算机）的静态 IP 地址为 192.168.1.23，您希望朋友能够通过默认端口 21 访问此服务器，且采用 TCP 协议，那么，请按照如下步骤进行设置：

1. 在图 5-36所示的“虚拟服务器”页面点击**添加新条目**按钮。
2. 按图 5-37所示进行设置。其中的服务端口号和协议，可以手动输入，也可以通过在“常用服务端口号”中选择“FTP”，使其对应的端口号“21”和协议“TCP”自动填入到相应设置框中。
3. 单击**保存**按钮，可以看到设置完成后的虚拟服务列表如图 5-36所示。

当您的朋友访问此 FTP 服务器时，只需在浏览器中输入 ftp://xxx.xxx.xxx.xxx:21 即可。其中，“xxx.xxx.xxx.xxx”是本路由器的 WAN 口 IP 地址，如：当路由器 WAN 口 IP 为 172.32.90.1 时，需在浏览器中输入 ftp://172.32.90.1:21。

☞ 注意：

如果设置了服务端口为80的虚拟服务器，则需要将**安全设置→远端WEB管理**的“WEB管理端口”设置为80以外的值，如88，否则会与路由器远程服务端口发生冲突，因特网用户对此端口的访问将默认为对路由器的访问，而不会转到局域网服务器上，从而导致虚拟服务器不起作用。

5.9.2 特殊应用程序

特殊应用程序功能，可以使某些需要多条连接的应用程序，如 Internet 网络游戏、视频会议、网络电话等能够与网络服务器建立正常连接。

对于此类特殊的应用程序，在客户端向因特网服务器主动发起连接的同时，也需要服务器向客户端发起连接。但在缺省情况下，因特网服务器向局域网客户端发起的连接请求都会被路由器拒绝，导致连接中断。

通过设置**特殊应用程序**，当局域网中有此类请求时，应用程序向触发端口发起连接，会触发路由器打开所有开放端口来为正常连接提供保证。

选择菜单**转发规则→特殊应用程序**，可以在图 5-38所示界面中查看和编辑特殊应用程序条目。



ID	触发端口	触发协议	开放端口	开放协议	状态	编辑
1	7175	ALL	51200-51201,51210	ALL	生效	编辑 删除
2	6112	ALL	6112	ALL	生效	编辑 删除

图 5-38 特殊应用程序

点击**添加新条目**按钮，可以在下图 5-39所示界面中设置新的特殊应用程序条目。

特殊应用程序

某些程序需要多条连接，如Internet游戏，视频会议，网络电话等。由于防火墙的存在，这些程序无法在简单的NAT路由下工作。特殊应用程序使得某些这样的应用程序能够在NAT路由下工作。

触发端口： 7175

触发协议： ALL

开放端口： 51200-51201,51210

开放协议： ALL

状态： 生效

常用应用程序： Dialpad

保 存　返 回　帮 助

图 5-39 设置特殊应用程序条目

触发端口： 该端口是应用程序首先发起连接的端口，只有在该端口上发起连接，开放端口中的所有端口才可以开放。

触发协议： 触发端口上使用的协议，可选项有 TCP、UDP 和 ALL。若对采用的协议不清楚，推荐选择 ALL。

开放端口： 当应用程序向触发端口上成功发起连接后，触发对应的开放端口，因特网服务器可通过开放端口与内网计算机连接。可输入单个端口值或端口段。端口段输入格式为“开始端口-结束端口”，不同的端口段用“,”隔开。

开放协议： 开放端口上使用的协议，可选项有 TCP、UDP 和 ALL。若对采用的协议不清楚，推荐选择 ALL。

状态： 设置该条目是否生效。只有状态为生效时，本条目的设置才有效。

常用应用程序： 选择需要设置的应用程序，系统会自动将该应用程序的触发端口号和开放端口号添加到上述对应项中。对于“常用应用程序”中没有列出的程序，需要手动输入触发端口和开放端口的相关信息。

5.9.3 DMZ主机

局域网中设置 DMZ（Demilitarized Zone，非军事区）主机后，该主机将完全暴露给广域网，可以实现双向无限制通信。

DMZ 主机实际上就是一个开放了所有端口的虚拟服务器，当需要设置的虚拟服务器的开放端口不确定时，可以把它设置成 DMZ 主机。

选择菜单**转发规则→DMZ主机**，可以在图 5-40所示界面中设置DMZ主机。

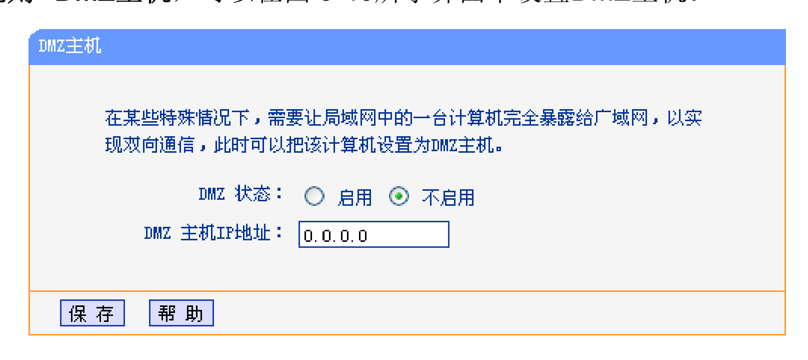


图 5-40 DMZ 主机

DMZ 状态： 选择是否启用 DMZ 主机功能。

DMZ 主机 IP 地址： 输入要设置为 DMZ 主机的局域网计算机的静态 IP 地址。

完成设置后，点击**保存**按钮。

因特网用户访问DMZ主机的方法与访问虚拟服务器的方法一样，具体可参考5.9.1 虚拟服务器的“举例”部分。

☞ 注意：

1. 添加DMZ主机可能会给该主机带来不安全因素，因此不要轻易使用这一选项。
2. DMZ主机的优先级低于虚拟服务器，因特网用户对路由器同一端口的访问将优先转发到虚拟服务器所对应的局域网服务器上。

5.9.4 UPnP设置

依靠 UPnP(Universal Plug and Play，通用即插即用)协议功能，局域网中的主机可以请求路由器自动进行端口转换，使得外部主机能够在需要时访问内部主机上的资源，如 Windows XP 和 Windows ME 系统上安装的 MSN Messenger 或迅雷、BT、PPLive 等支持 UPnP 协议的应用程序。

选择菜单**转发规则→UPnP设置**，可以在图 5-41所示界面中查看UPnP信息。

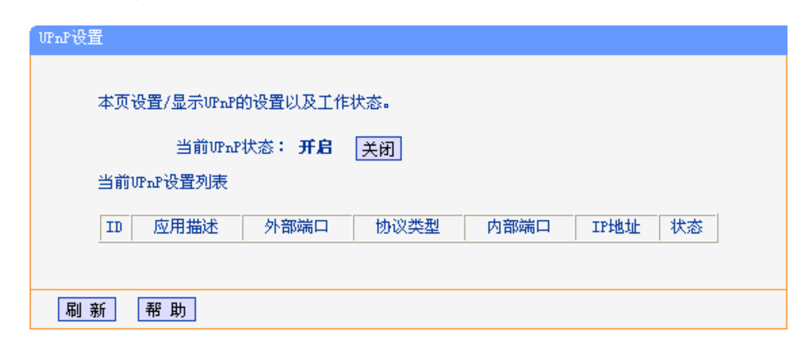


图 5-41 UPnP 设置

应用描述： 显示应用程序通过 UPnP 向路由器请求端口转换时给出的描述。

外部端口： 显示端口转换时使用的路由器端口号。

协议类型： 显示进行端口转换时采用的协议类型。

内部端口： 显示需要进行端口转换的局域网主机端口号。

IP 地址： 显示需要进行端口转换的局域网主机 IP 地址。

状态： 显示该条目是否已经启用。

使用时点击**开启**按钮即可，端口转换信息由应用程序发出请求时提供，无需进行任何设置。点击**刷新**按钮可以看到当前正在使用本功能的应用程序的端口转换相关信息，如图 5-41。

☞ 注意：

1. 因为现阶段版本的UPnP协议的安全性还未得充分保证，不使用时请关闭UPnP功能。
2. 只有支持UPnP协议的应用程序才能使用本功能。
3. UPnP功能需要操作系统的支持(如Windows ME/Windows XP/Windows Vista/Windows 7)。

5.10 安全功能

路由器的"安全功能"用于保障网络的安全。"安全设置"和"高级安全设置"可以有效抵御一些常见的网络攻击，为网络安全提供保障措施；"局域网 WEB 管理"可以限制局域网内主机访问路由器的 WEB 管理界面；而"远端 WEB 管理"又为广域网用户执行远程管理提供了可能。

选择菜单**安全功能**，可以看到：

- 安全功能
  - 安全设置
  - 高级安全设置
  - 局域网WEB管理
  - 远端WEB管理

单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.10.1 安全设置

选择菜单**安全功能→安全设置**，可以在下图 5-42界面中设置是否启用路由器的基本安全功能。

安全设置

本页对各个基本安全功能的开启与关闭进行设置。

状态检测防火墙 (SPI)

SPI 防火墙： ⦿ 启用 ○ 不启用

虚拟专用网络 (VPN)

PPTP 穿透： ⦿ 启用 ○ 不启用

L2TP 穿透： ⦿ 启用 ○ 不启用

IPSec 穿透： ⦿ 启用 ○ 不启用

应用层网关 (ALG)

FTP ALG： ⦿ 启用 ○ 不启用

TFTP ALG： ⦿ 启用 ○ 不启用

TFTP ALG： ⦿ 启用 ○ 不启用

RTSP ALG： ⦿ 启用 ○ 不启用

保 存 帮 助

图 5-42 安全设置

状态检测防火墙（SPI）： 开启时，只有内网主动发起的请求才可以建立连接，所有来自外网的主动请求均被防火墙拒绝，从而能够保证内网免受来自外网的恶毒攻击，保护内网的安全。推荐保持默认状态"启用"。

虚拟专用网络（VPN）： VPN为远程计算机通过广域网进行安全通信提供了方法。如果内网主机需要使用VPN协议(如PPTP、L2TP、IPSec)通过路由器连接到远程VPN网络，那么应开启相应的VPN穿透功能。

应用层网关（ALG）： ALG为某些采用"控制/数据"模式的应用层协议（如FTP、TFTP、H323等）在通过NAT网关时作网络地址和端口的转换。推荐保持默认状态"启用"。

完成设置后，点击**保存**按钮。

5.10.2 高级安全设置

选择菜单**安全功能→高级安全设置**，可以在下图 5-43界面中开启DoS(拒绝服务)攻击防范并设置相关参数。

DoS 攻击的目的是用极大量的虚拟信息流耗尽目标主机的资源。受害者被迫全力处理虚假信息流，从而影响对正常信息流的处理。如果 DoS 攻击始发自多个源地址，则称为分布式拒绝服务(DDoS)攻击。通常 DoS 与 DDoS 攻击中的源地址都是欺骗性的。开启 DoS 攻击防范后，若某主机向目标主机发送某种数据包的速率大于您所设置的值，那么该主机将被列入"DoS 被禁主机列表"而不能上网，从而很好地防止了 DoS 攻击。

高级安全选项

注意：
1、只有启用了“DOS攻击防范”，后面的设置才能够生效。
2、这里“数据包统计时间间隔”与“系统工具” – “流量统计”中的“数据包统计时间间隔”为同一值，无论在哪一个模块进行修改都会覆盖另一模块里的数值。
3、由于“DoS攻击防范”的部分功能是以相关数据包的统计为依据的，因此，如果“系统工具” - “流量统计”中的流量统计功能被关闭，那么将会导致这部分功能失效。

数据包统计时间间隔（5~60）： 10 秒

DoS攻击防范： ○ 不启用 ◉ 启用

☐ 开启ICMP-FLOOD攻击过滤
ICMP-FLOOD数据包阀值（5~3600）： 50 包/秒

☐ 开启UDP-FLOOD过滤
UDP-FLOOD数据包阀值（5~3600）： 500 包/秒

☐ 开启TCP-SYN-FLOOD攻击过滤
TCP-SYN-FLOOD数据包阀值（5~3600）： 50 包/秒

☐ 忽略来自WAN口的Ping
☐ 禁止来自LAN口的Ping包通过路由器（防范冲击波病毒）

保 存 | DoS 被禁主机列表 | 帮 助

图 5-43 高级安全选项

数据包统计时间间隔： 设置对数据包进行统计的时间间隔。如果统计得到发往同一目标IP地址的某种数据包(例如UDP FLOOD)达到了指定的阈值，那么系统将认为UDP-FLOOD攻击已经发生。如果UDP-FLOOD过滤已经开启，那么路由器将会停止接收该类型的数据包，从而达到防范攻击的目的。此处的值和**系统工具→流量统计**中的“数据包统计时间间隔”是一样的，一处的更改将引起另一处作同样的更改。

DoS攻击防范： 该项是开启下面各种攻击防范的总开关，只有选择此项后，以下的几种防范措施才能生效。

开启ICMP-FLOOD攻击过滤： 若需要防范ICMP-FLOOD攻击，请选择此项。

ICMP-FLOOD数据包阈值： 当开启ICMP-FLOOD功能后，如果在指定时间间隔内发往同一目标IP地址的ICMP包达到了设定值，防范措施将立即启动。

开启UDP-FLOOD攻击过滤： 若需要防范UDP-FLOOD，请选择此项。

UDP-FLOOD数据包阈值： 当开启UDP-FLOOD功能后，如果在指定时间间隔内发往同一目标IP地址的UDP包达到了设定值，防范措施则立即启动。

开启TCP-SYN-FLOOD攻击过滤：

若需要防范TCP-SYN-FLOOD，请选择此项。

TCP-SYN-FLOOD数据包阈值：

当开启TCP-SYN-FLOOD功能后，如果在指定时间间隔内发往同一目标IP地址的TCP的SYN包达到了设定值，防范措施则立即启动。

忽略来自WAN口的Ping： 若开启该功能，广域网的计算机将不能Ping通路由器。

禁止来自LAN口的Ping包通过路由器：

若开启该功能，局域网的计算机将不能Ping通广域网中的计算机。

DoS被禁主机列表： 点击该按钮，你可以查看被禁止的主机列表，如图5-44。单击**刷新**按钮可以更新列表信息。若希望被禁主机能够重新上网，可以点击**删除**按钮；若需要释放所有被禁主机，可以点击**清空**按钮。

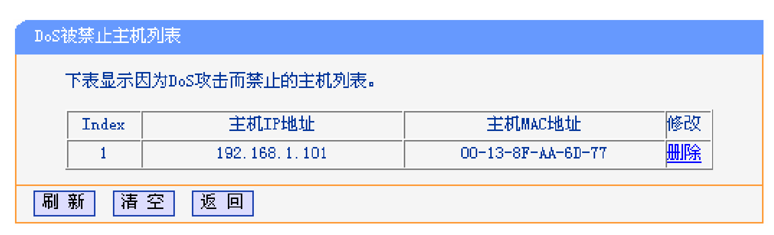


图 5-44 DoS 被禁主机列表

完成更改后，点击**保存**按钮。

☞ 注意：

只有在开启了**系统工具→流量统计**中的流量统计功能后，DoS 攻击防范才能正常生效。

5.10.3 局域网WEB管理

选择菜单**安全功能→局域网WEB管理**，可以在下图 5-45界面中设置允许访问此WEB页面的局域网计算机的MAC地址。

局域网WEB管理

本页设置局域网中可以执行WEB管理的计算机的MAC地址。

○ 允许所有内网主机访问本WEB管理页面

⦿ 仅允许列表中的MAC地址访问本WEB管理页面

MAC地址 1： 00-19-66-80-54-37

MAC地址 2： 00-16-28-45-23-85

MAC地址 3：

MAC地址 4：

当前管理PC的MAC地址： 6c-62-6d-f7-32-44 添 加

注意：您可以通过按下路由器上的复位按钮将路由器的所有设置恢复到出厂时的默认状态。

保 存 帮 助

图 5-45 局域网 WEB 管理

如果允许局域网中的所有计算机访问此WEB页面，请保持默认设置“允许所有内网主机访问本WEB管理页面”；如果只允许局域网中的部分计算机访问此WEB页面，请选择“仅允许列表中的MAC地址访问本WEB管理页面”，并将允许的计算机的MAC地址添加到列表中。单击**添加**按钮还可以把当前正在访问此WEB页面的计算机的MAC地址复制到列表中。

完成设置后，点击**保存**按钮。

☞ 注意：

如果选择了“仅允许列表中的MAC地址访问本WEB管理页面”，而没有把当前管理PC的MAC地址加入到列表中，那么当点击**保存**按钮以后，将无法继续通过当前PC来管理本路由器。在这种情况下，如果想重新获得对路由器的控制权，请将路由器恢复到出厂设置（如何恢复请参考3.2复位）。

5.10.4 远端WEB管理

远端 WEB 管理功能允许用户通过 Web 浏览器（如 Internet Explorer 等）从广域网登录此管理页面配置管理路由器。

选择菜单**安全功能→远端WEB管理**，可以在下图 5-46界面中设置远程管理主机的IP地址和登录端口。

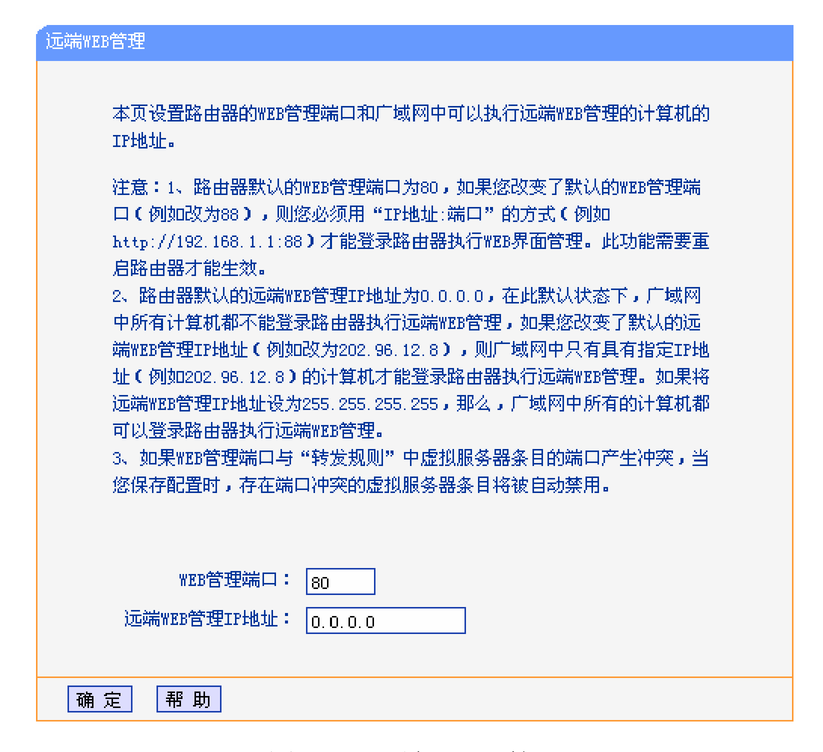


图 5-46 远端 WEB 管理

WEB管理端口： 用于访问宽带路由器的WEB管理端口号。路由器默认的WEB管理端口为80，如果改变了默认的WEB管理端口(例如改为88)，则必须用“http://IP地址:端口”的方式(例如http://192.168.1.1:88)才能登录路由器执行WEB界面管理。此功能需要重启路由器后才生效。

远端WEB管理IP地址： 广域网中可以访问该路由器执行远端WEB管理的计算机IP地址。路由器默认的远端WEB管理IP地址为0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端WEB管理。如果改变了默认的远端WEB管理IP地址，则广域网中只有具有该指定IP地址的计算机才能登录路由器执行远端WEB管理。如果改为255.255.255.255，则广域网中所有主机都可以登录路由器执行远端WEB管理。

完成更改后，点击**保存**按钮。

举例：如果您想让朋友帮忙设置路由器的某项功能，而这位朋友不在本地。那么，可以通过“远端WEB管理”使其从广域网访问本路由器的管理页面。假如您朋友计算机的IP地址为202.96.134.13，想通过默认管理端口80登录本路由器。那么，请进行如下设置：

1. 在图 5-46页面设置“WEB管理端口”为“80”。
2. 在图 5-46页面的“远端WEB管理IP地址”处输入“255.255.255.255”或“202.96.134.13”。

这样，您朋友只需在他自己计算机的Web浏览器地址栏处输入您路由器WAN口IP地址即可访问您路由器的管理界面并进行设置。

☞ 注意：

路由器的WAN口IP地址可在路由器的**运行状态**页面查询。

5.11 家长控制

通过**家长控制**功能，可以对小孩的上网时间和访问的网站进行控制。

家长控制功能使您可以选择局域网中的一台 PC（Personal Computer，即个人电脑）作为家长 PC，家长 PC 可以不受限制地正常上网，而其他所有 PC 只能根据控制列表中的规则在指定的时间访问指定的网站。若某台非家长 PC 不在控制列表中，则此 PC 将无法上网。

家长控制只能使局域网中的一台PC不受控制，而且受控PC能够访问的网站数量很有限。若想放宽受控条件，如使更多的PC不受控制或使受控PC能访问更多的网站，那么请参阅5.12 上网控制部分。

选择菜单**家长控制**，可以在下图 5-47界面中设置家长控制条目。



图 5-47 家长控制设置

家长控制： 选择是否开启家长控制功能。开启此功能后，只有家长PC可以正常上网，其他PC均会受到控制。

家长PC的MAC地址：

设定家长PC，即不受控制的PC的MAC地址。

当前管理PC的MAC地址：

此处显示当前正在操作的PC的MAC地址，单击其后的**设为家长PC**按钮可以把此MAC地址复制到"家长PC的MAC地址"一栏中。

完成更改后，点击**保存**按钮使设置生效。

单击**增加单个条目**按钮，可以在下图5-48界面中设置家长控制条目。

家长控制规则设置

本页设置一条家长控制条目。

本页面中的日程计划基于路由器的系统时间，您可以在 “系统工具-> 时间设置 ” 中查看和设置系统时间。

小孩PC的MAC地址： 6C-62-6D-F7-32-44

当前局域网中PC的MAC地址： 6C-62-6D-F7-32-44(192.168.1.100)

给允许的网站列表一个描述： 雅虎&谷歌

允许小孩访问的网站域名： www.yahoo.com.cn

www.google.com.cn

希望在哪些时候生效： 周六全天

您可以在 “上网控制-> 日程计划 ” 中设置时间列表

状态： 生效

保 存 返 回 帮 助

图 5-48 家长控制规则设置

小孩 PC 的 MAC 地址：

受控制的 PC 的 MAC 地址，为空则表示对局域网中所有的非家长 PC 应用此控制规则。

当前局域网中 PC 的 MAC 地址：

此处列出了当前局域网中所有 PC 的 MAC 地址及其对应的 IP 地址，可通过 IP 地址选择想要控制的一台 PC，选择后该 PC 对应的 MAC 地址会自动复制到“小孩 PC 的 MAC 地址”一栏中。

给允许的网站列表一个描述：

为便于识别，请在此处输入对允许小孩访问的网站列表的一个简单描述，不同控制条目的描述不能相同。

允许小孩访问的网站域名：

可以填写 8 个允许的网站完整域名或域名的关键字，如果您在此处填入某一个字符串（例如：yahoo），则含有该字符串的域名（www.yahoo.com、www.yahoo.com.cn）都可以被匹配。

希望在哪些时候生效：

允许小孩访问以上网站的时间段。如果已经在**上网控制→日程计划**中设置好了时间，请直接在下拉列表中选择，否则请先保存设置，然后单击**日程计划**进入日程计划设置对话框进行设置。有关日程计划的设置请参阅本文档5.12.4 日程计划部分。

状态： 以上设置是否生效。

完成更改后，点击**保存**按钮。

举例：假如家长PC的MAC地址为00-19-66-80-54-37，小孩PC的MAC地址为00-19-66-80-53-CF，为了不影响学习，希望小孩只能在周六全天及周日上午的8：00-11：30访问雅虎（www.yahoo.com.cn）及谷歌网站（www.google.com.cn），而家长自己不受任何控制，那么请按以下步骤进行设置：

1. 在“家长控制”中启用家长控制功能；若“当前管理 PC 的 MAC 地址”为00-19-66-80-54-37，则点击**设为家长 PC** 按钮，否则手动填入家长 PC 的 MAC 地址“00-19-66-80-54-37”。

2. 在**上网控制→日程计划**中添加两条新的日程计划，分为命名为“周六全天”、“周日上午”，时间分别设置为“星期六、全天-24 小时”、“星期天、开始时间：0800、结束时间：1130”。设置保存后的结果如下图 5-49所示。



图 5-49 日程计划设置示例

3. 返回“家长控制设置”界面，点击**增加单个条目**按钮，按图 5-48所示进行设置。

4. 保存设置。重复第 3 步，并将第 3 步中的“给允许的网站列表一个描述”改为“雅虎&谷歌_2”、“希望在哪些时候生效”改为“周日上午”，点击**保存**按钮。

完成以上设置之后，看到的规则列表将是：

ID	MAC 地址	网站列表	日程计划	状态	配置
1	00-19-66-80-53-CF	雅虎&谷歌_1	周六全天	生效	编辑 删除
2	00-19-66-80-53-CF	雅虎&谷歌_2	周日上午	生效	编辑 删除

5.12 上网控制

通过上网控制功能，可以控制局域网内主机的上网行为，使其上网时间和访问的网站受到一定规则的限制，如控制某台主机只能在某个时段登录某些网站，或在某个时间段不能登录这些网站等。

与**家长控制**相比，**上网控制**功能显得更灵活。**上网控制**可以通过一台主机控制一台或几台局域网内的其他主机。如果您的家中有小孩，上网控制和家长控制功能都可以有效的控制小孩的上网范围和上网时间，使小孩能够更健康的使用互联网。但上网控制的应用更为广泛，如果您家有三台电脑，那么**上网控制**功能可以在控制小孩使用电脑的同时对另两台电脑不作控制。

选择菜单**上网控制**，可以看到：



单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.12.1 规则管理

通过规则管理，可以设置和管理局域网内主机上网的规则，允许或禁止"主机列表"中的主机在"日程计划"时间段内访问"访问目标"网站。

选择菜单**上网控制→规则管理**，可以在下图5-50所示面中设置对内网主机上网行为的控制规则。



图 5-50 上网控制规则管理

开启上网控制： 选中则开启上网控制功能，若不选中则规则无效。

缺省过滤规则： 凡是符合已设上网控制规则的数据包，允许通过本路由器--选择此项，则凡是符合上网控制规则的数据包，均可以通过本路由器。

凡是符合已设上网控制规则的数据包，禁止通过本路由器--选择此项，则凡是符合所设上网控制规则的数据包，均不能通过本路由器。

移动： 通过该按钮来调整各条控制规则的顺序，以达到不同的控制优先级(ID序号越靠前则优先级越高)。

完成更改后，点击**保存**按钮。

点击**增加单个条目**按钮，可以在下图5-51界面中设置新的上网控制条目。



图 5-51 上网控制规则设置

规则描述： 对该上网控制条目的简单描述，此描述必须是唯一的，如"周末 8：00-12：00"，用于标识所设的上网规则。

主机列表： 此条目为要控制的内网主机。如果已经在**上网控制→主机列表**中设置好了要控制的主机的信息，请直接在下拉列表中选择，否则请单击**点击此处添加主机列表**进入主机列表设置对话框进行设置。有关主机列表的设置请参阅本文档5.12.2 主机列表部分。

访问目标： 允许或禁止"主机列表"中的主机访问的网站域名或IP地址。如果已经在**上网控制→访问目标**中设置好了访问目标信息，请直接在下拉列表中选择，否则请单击**点击此处添加访问目标**进入访问目标设置对话框进行设置。有关访问目标的设置请参阅本文档5.12.3 访问目标部分。

日程计划： 允许或禁止"主机列表"中的主机访问目标网站的时间段。如果已经在**上网控制→日程计划**中设置好了时间，请直接在下拉列表中选择，否则请单击**点击此处添加日程计划**进入日程计划设置对话框进行设置。有关日程计划的设置请参阅本文档5.12.4 日程计划部分。

生效： 该上网控制条目是否生效。

完成更改后，点击**保存**按钮。

举例： 周一到周五为小明学习的时间，在此期间有必要禁止他的电脑上网。因此，需要限制局域网中IP地址为192.168.1.88的计算机（该计算机的主人为小明）只能在周末上网，而局域网中的其它主机（假设IP地址为192.168.1.89-192.168.1.91）不受任何控制，请按照以下步骤进行设置：

1. 在**主机列表**中添加两个条目，其一：主机名为"小明的计算机"，IP地址为192.168.1.88；其二：主机名为"其他计算机"，IP地址为192.168.1.89-192.168.1.91。
2. 在**日程计划**设置中，输入日程描述"周末全天"，勾选"星期六"、"星期天"和"全天-24小时"，如图5-52，单击**保存**完成设置。

增加或修改日程计划设置

本页可以增加或修改一条日程计划规则，日程计划基于路由器的时间。

日程描述： 周末全天

星期： 每天 选择星期

星期一 星期二 星期三 星期四 星期五

星期六 星期天

时间： 全天-24小时

开始时间： （HHMM）

结束时间： （HHMM）

保 存 返 回 帮 助

图 5-52 日程计划设置

3. 回到图5-50所示的“上网控制规则管理”界面，启用上网控制功能，选择缺省过滤规则为“凡是不符合已设上网控制规则的数据包，禁止允许通过本路由器”，点击**保存**按钮。
4. 单击**增加单个条目**按钮，按下图进行设置并保存。

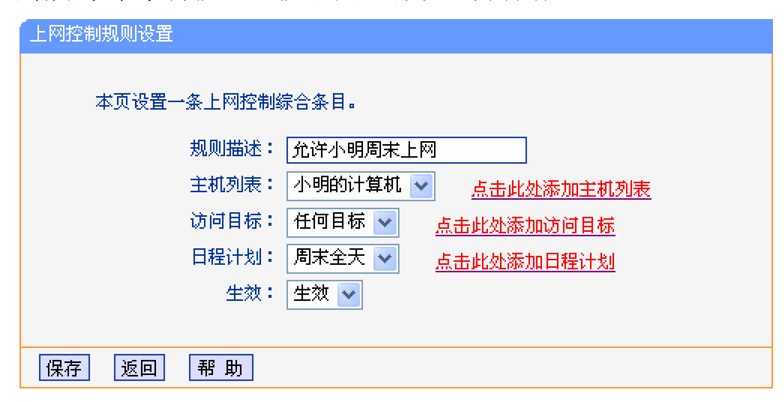


图 5-53 上网控制规则设置示例一

5. 再次在图5-50所示界面中点击**增加单个条目**按钮，按下图5-54所示进行设置并保存。

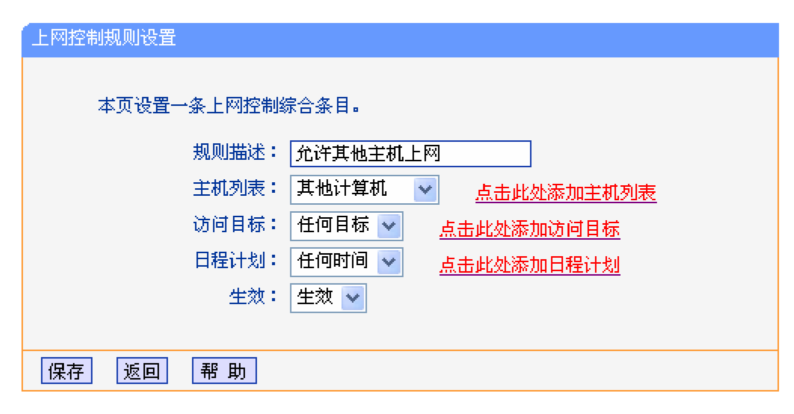


图 5-54 上网控制规则设置示例二

完成以上设置之后，可以看到下图所示的规则列表：

ID	规则描述	主机列表	访问目标	日程计划	生效	配置
1	允许小明周末上网	小明的计算机	任意	周末全天	☑	编辑 删除
2	允许其他主机上网	其他计算机	任意	永久	☑	编辑 删除

5.12.2 主机列表

主机列表列举了需要遵守上网控制规则的主机信息，包括主机名，主机信息等。在主机列表设置中，可以增加，编辑和删除相应的主机列表。

选择菜单**上网控制→主机列表**，可以在下图5-55界面中设置受控的内网主机列表。



图 5-55 主机列表设置

单击**增加单个条目**按钮，可以在下图 5-56界面中设置新的受控主机信息。

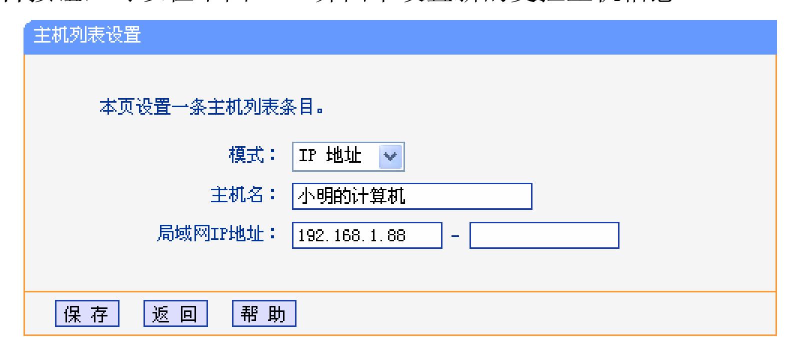


图 5-56 主机列表设置示例

模式： 选择标识受控主机身份的模式，有IP地址和MAC地址两个选项。

主机名： 给受控主机的一个简单描述，不同主机列表条目中的主机名不能相同。

局域网IP地址：

如果选择的模式为IP地址，请在此输入一台受控主机的IP地址或IP地址连续的多台受控主机的首尾IP地址。如果选择的模式为MAC地址，请在此输入受控主机的MAC地址。

完成更改后，点击**保存**按钮。此时图 5-55所示界面的列表中将显示刚刚设置的主机条目的信息。

单击**删除所有条目**按钮，可以一次性删除列表中的所有条目。删除所有条目后，则原先设置的上网控制规则对相应主机失效。

5.12.3 访问目标

访问目标显示了主机上网访问的目标网站或目标 IP 地址，如“www.baidu.com”，“192.168.1.71”等。

选择菜单**上网控制→访问目标**，可以在下图5-57界面中设置允许或禁止受控主机访问的目标信息。



图 5-57 访问目标设置

单击**增加单个条目**按钮，可以在下图 5-58界面中设置新的访问目标的信息。

访问目标列表设置

本页设置一条访问目标列表条目。

模式：IP 地址

目标描述：百度

目标IP地址：202.108.22.5 -

目标端口：80 -

协 议：TCP

常用服务端口号：HTTP

保 存 返 回 帮 助

图 5-58 访问目标列表设置—IP 地址模式

请选择模式： 选择描述访问目标信息的模式，有IP地址和网站域名两个选项。如果选择了网站域名模式，此设置页面将如图5-59所示。

目标描述： 给访问目标的一个简单描述，此描述必须是唯一的。

目标IP地址： 输入一个访问目标的IP地址或连续的访问目标IP地址段。

目标端口： 允许或限制访问的目标IP地址的服务端口，可以为一个端口号或连续的端口段。如果不清楚目标端口号，可以在"常用服务端口号"的下拉列表中通过选择服务来自动填入。

协议： 访问目标的服务器所使用的协议。如果不清楚采用的协议，推荐选择ALL。

常用服务端口号： 下拉列表中列举了一些常用的服务端口，从中选择需要的服务，则该服务对应的端口号会自动填入上面的"目标端口"输入框中。

访问目标列表设置

本页设置一条访问目标列表条目。

模式：网站域名

目标描述：百度

网站域名：

保 存 返 回 帮 助

图 5-59 访问目标列表设置—网站域名模式

网站域名： 在域名模式下，可以为列表设置4个网站完整域名或域名的关键字，如果在此处填入某一个字符串（例如：yahoo），则含有该字符串的域名（www.yahoo.com、www. yahoo.com.cn）都可以被匹配。

完成更改后，点击**保存**按钮。

5.12.4 日程计划

在"日程计划"中，可以设置上网规则生效的时间。此处的时间包括日期和时间段。日期可以为一个星期的某几天，也可以为每天。时间段可以设为某两个时间点间的时间段，也可以为"全天 24 小时"。

选择菜单**上网控制→日程计划**，可以在下图5-60界面中设置允许或禁止受控主机上网的时间段。

☞ 注意：

在设置之前，请确保路由器的时间是正确的，有关路由器的时间设置请参阅本文档5.17.1 时间设置部分。



图 5-60 日程计划设置

单击**增加单个条目**按钮，可以在下图 5-61界面中设置新的日程计划。

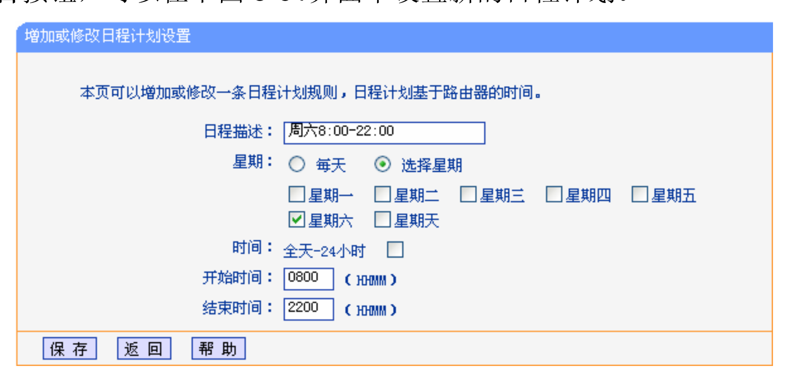


图 5-61 日程计划设置示例

日程描述： 给日程计划的简单描述，此描述必须是唯一的，例如"周末8：00-20：00"。

星期： 点选"每天"，可以将时间设置为每天，点选"选择星期"，则可将时间设置为每个星期的某几天。

时间： 如果想设置为全天，请直接选择"全天-24小时"，否则请在开始时间、结束时间中输入要设置的具体时间，注意时间格式为HHMM，即前两位为小时，后两位为分钟。

完成更改后，点击**保存**按钮。

5.13 路由功能

选择菜单**路由功能**，可以看到：

- 路由功能
  - 静态路由表
  - 系统路由表

5.13.1 静态路由表

单击**静态路由表**，即可进行静态路由功能设置，下面将详细讲解静态路由功能的设置。

静态路由是一种特殊的路由，由网络管理员手动配置。在网络中使用合适的静态路由可以减少路由选路造成的网络开销，提高数据包的转发速度。

静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

通过设定目的 IP 地址、子网掩码和网关地址可以确定一个路由条目。其中目的 IP 地址和子网掩码用来确定一个目标网络/主机，然后路由器会将数据包发往相应静态路由条目的网关，并由该网关转发数据包。

☞ 注意：

当路由器周围的网络环境较复杂，或者您没有完全了解周围网络的拓扑结构时，请慎用此功能。

选择菜单**路由功能→静态路由表**，可以在下图 5-62的界面中设置静态路由信息。



图 5-62 静态路由表

点击**添加新条目**按钮，你可以在下图中添加静态路由条目。如图 5-63。



图 5-63 添加静态路由条目

目的 IP 地址： 用来标识希望访问的目标地址或目标网络，此 IP 地址不能和路由器的 WAN 口或 LAN 口 IP 地址处于同一网段。

子网掩码： 该项与目的 IP 地址一起来标识目标网络。

默认网关： 数据包被指定发往的下一个节点的 IP 地址，此 IP 地址必须和路由器的 WAN 口或 LAN 口 IP 地址处于同一网段。

状态： 显示该条目是否生效。只有状态为生效时，此路由条目才起作用。

5.13.2 系统路由表

系统路由表显示了所有正在使用的路由表条目，如图 5-64所示，每条路由表条目由目的IP地址，子网掩码，网关和网络接口组成。点击刷新按钮可以刷新路由表。



图 5-64 系统路由表

目的网络地址： 静态路由条目所指定的目的主机或网络的网络地址。

子网掩码： 子网掩码决定了目的 IP 地址的网络号和主机号。

网关： 连接路由器和目的主机或网络的网关设备的网络地址。

接口： 网络接口显示目的 IP 地址位于 LAN 与 WLAN(内部有线和无线网络)，或者 WAN(外部网络)。

5.14 IP带宽控制

带宽控制功能可以实现对局域网计算机上网带宽的控制。在带宽资源不足的情况下，通过对各类数据包的带宽进行控制，可以实现带宽的合理分配，达到有效利用现有带宽的目的。通过 IP 带宽控制功能，可以设置局域网内主机的带宽上下限，保证每台主机都能通畅地共享网络，并在网络空闲时充分利用网络带宽。

选择菜单 **IP 带宽控制**，可以看到：

- IP带宽控制
  - 控制设置
  - 控制规则

单击菜单中的子项即可进行具体的设置，下面将详细讲解各子项的功能和设置方法。

5.14.1 控制设置

带宽设置分为“上行总带宽”和“下行总带宽”。上行总带宽是指所有内网计算机同时上传数据时占用的总带宽，由 ISP 提供的大小决定。下行总带宽则指所有内网计算机同时下载数据时占用的总带宽。通常 ISP 提供的带宽指的是“下行总带宽”，如“1M”等。通过**控制设置**，我们可以对上行，下行总带宽分别进行设置。

选择**IP带宽控制→控制设置**，可以进入下图 5-65所示界面。本页主要对IP带宽控制的开启与关闭进行设置。



图 5-65 IP 带宽控制设置功能设置

开启IP带宽控制：

选择是否开启IP带宽控制功能，只有此处开启时，后续的“控制规则”设置才能够生效。

选择带宽类型：

选择带宽线路类型。

上行总带宽： 输入希望路由器通过WAN口提供的上传速率，最大值为1000000Kbps。

下行总带宽： 输入希望路由器通过WAN口提供的下载速率，最大值为1000000Kbps。

☞ 注意：

为了使IP带宽控制达到最佳效果，请设置正确的线路类型，并向ISP了解线路的上行/下行总带宽。

5.14.2 控制规则

在控制规则中，可以设置局域网计算机的上下行带宽参数，满足局域网中每台主机的上网需求。选择**IP带宽控制→控制规则**，将进入下图 5-66所示界面。控制规则分为控制规则列表和控制规则配置。



图 5-66 IP 带宽控制规则列表

ID： 规则序号。

描述： 显示描述的信息，包括地址段，传输层的端口段和协议。

上行带宽： 表示主机发送数据时占用的带宽，此处显示WAN口允许的最大上传速度限制和最小上传速度保证，为0时表示采用缺省值。输入范围为0-1000000Kbps。

下行带宽：　　表示主机接受数据时占用的带宽，此处显示WAN口允许的最大下载速度限制和最小下载速度保证，为0时表示采用缺省值。输入范围为0-1000000Kbps。

启用：　　显示规则的状态，选中该复选框则表示该规则生效。

配置：　　对相应的规则进行编辑或删除。

点击控制规则列表中的**添加新条目**或**编辑**按钮，可以进入图5-67设置界面。在控制规则配置中，可以创建新的IP带宽控制规则或修改已存在的规则，配置结果将在图5-66中显示。



图 5-67 带宽控制规则配置

启用：　　选择是否启用该规则。

IP地址段：　　输入内部主机的地址范围。当全部为空或为0.0.0.0时表示该域无效。

端口段：　　通过设置端口段，可以限制主机访问网络的端口范围。一般浏览网页的端口为“80”，而登录QQ的端口则为1500左右。可以在此输入内部主机访问外部服务器的端口范围，当全部为空或为0时表示该域无效。普通用户可以不用设置“端口段”。

协议：　　输入传输层采用的协议类型，这里有ALL(任意匹配)、TCP和UDP；该域只有在端口段选中下才有效。

上行带宽、下行带宽：　　上行带宽表示主机发送数据时占用的带宽，下行带宽则表示主机接受数据时占用的带宽。通常，上行带宽远远小于下行带宽，下行带宽的设置则需参考总带宽和主机数量，以及内网计算机的上网需求。

5.15 IP与MAC绑定

IP 与 MAC 绑定，可以有效防止 ARP 攻击，维护局域网用户的上网安全。

选择菜单 **IP 与 MAC 绑定**菜单，可以看到：

- IP与MAC绑定
  - 静态ARP绑定设置
  - ARP映射表

单击菜单中的子项即可进行具体的设置，下面将详细讲解两个子项的功能和设置方法。

5.15.1 静态ARP绑定设置

静态 ARP 绑定，即 IP 与 MAC 绑定，是防止 ARP 攻击本路由器的有效方法。

路由器在局域网内传输 IP 数据包时是靠 MAC 地址来识别目标的，因此 IP 地址与 MAC 地址必须一一对应，这些对应关系靠 ARP 映射表来维护。ARP 攻击可以用伪造的信息更新路由器的 ARP 映射表，破坏表中 IP 地址与 MAC 地址的对应关系，使路由器无法与相应的主机进行通信。

静态 ARP 绑定将主机的 IP 地址与相应的 MAC 地址进行绑定，可以有效防止 ARP 列表被错误的 IP MAC 对应信息更替。

选择菜单**IP与MAC绑定→静态ARP绑定设置**，可以在图 5-68所示界面中设置静态ARP绑定条目。



图 5-68 静态 ARP 绑定设置

ARP绑定： 选择是否开启ARP绑定功能，只有选择"启用"并单击**保存**后，列表中的设置才能生效。

点击**增加单个条目**按钮，可以在图 5-69所示界面中设置新的静态ARP绑定条目。

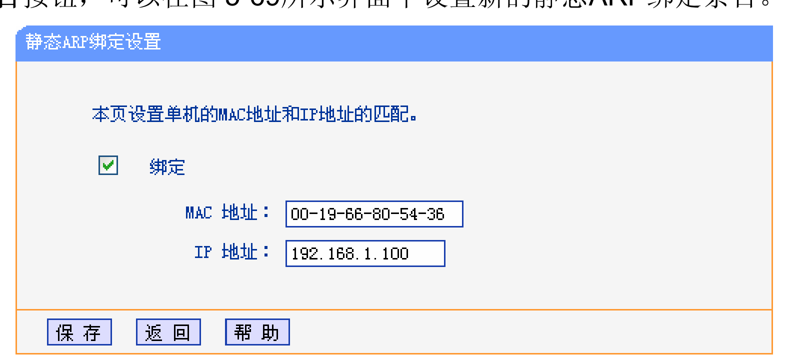


图 5-69 添加静态 ARP 绑定条目

绑定： 设置本条目状态，只有选中该项，该条绑定条目才能生效。

MAC 地址： 输入被绑定主机的 MAC 地址。

IP 地址： 输入被绑定主机的 IP 地址。

5.15.2 ARP映射表

如前所述，IP 数据包在局域网内传输时是靠 MAC 地址来识别目标的，IP 地址与 MAC 地址必须一一对应，ARP 映射表就是用来存储与维护这些对应信息的。

选择菜单**IP与MAC绑定→ARP映射表**，可以在图 5-70所示界面中查看ARP条目信息。



ARP映射表

ID	MAC地址	IP地址	状态	配置
1	00-0F-E2-80-30-90	172.31.70.1	未绑定	导入 删除
2	00-19-66-80-54-37	172.31.70.88	未绑定	导入 删除
3	00-19-66-80-54-36	192.168.1.100	未绑定	导入 删除

全部绑定 全部导入 刷 新 帮 助

图 5-70 ARP 映射表

导入： 将相应条目的ARP信息添加到图 5-68界面的静态ARP绑定列表中。

全部导入： 将当前ARP映射列表中所有条目的信息添加到图 5-68界面的静态ARP绑定列表中。

全部绑定： 将当前 ARP 映射列表中所有条目的状态设置为绑定，注意该按钮只有在启用了 ARP 绑定功能后才能点击。

☞ 注意：

1. 在进行导入操作时，如果该条目与ARP静态绑定表中的某条目有冲突，则会显示冲突提示，而且不会导入该条目。
2. 在进行全部导入操作时，如果同样存在冲突条目，则系统会忽略冲突条目，将其它没有冲突的条目添加到ARP静态绑定列表中。

举例：假如局域网内您计算机的静态 IP 地址为 192.168.1.100，MAC 地址为 00-19-66-80-54-36，为防止 ARP 攻击影响您计算机的正常通信，可以通过以下方法进行 ARP 绑定操作：

方法一：

1. 在图 5-68所示界面中启用ARP绑定并单击**保存**按钮。
2. 点击**增加单个条目**按钮。
3. 按图 5-69所示进行设置。
4. 单击**保存**按钮，可以看到设置完成后的ARP绑定条目如图 5-68所示。

方法二：

1. 在图 5-70所示界面中找到您的IP地址 192.168.1.100 和MAC地址 00-19-66-80-54-36 对应的条目，单击相应的**导入**按钮。
2. 返回图 5-68所示界面，在列表中选中导入条目对应的“绑定”。
3. 启用 ARP 绑定并单击**保存**按钮。

提示：

此处的ARP绑定只是在路由器上绑定了主机的IP MAC地址，因此只能使路由器免受ARP攻击。为保证上网安全，您还需在自己的计算机上绑定路由器LAN口的IP MAC地址，推荐使用ARP防火墙来实现此功能。

5.16 动态DNS

动态DNS又名DDNS，它的主要功能是实现固定域名到动态IP地址之间的解析。如果路由器的WAN口IP地址为动态获取的，通过此功能可使互联网上的其它主机用固定域名的方式访问您的路由器或虚拟服务器。

动态DNS功能对于使用动态IP地址的用户，在每次上网得到新的IP地址后，路由器内置的动态域名软件就会将该IP地址发送到由DDNS服务商提供的动态域名解析服务器，并更新域名解析数据库。当Internet上的其他用户需要访问这个域名的时候，动态域名解析服务器就会返回正确的IP地址。此功能对于大多数不使用固定IP地址的用户，也可以经济、高效地构建自身的服务网络。

选择菜单**动态DNS**，可以在图 5-71中设置动态DNS功能。只需在花生壳官方网站上进行注册，以相应的用户名/密码登录并启用DDNS功能即可。



图 5-71 动态 DNS 设置

服务商链接： 如果你还未在DDNS上注册，请选择“花生壳动态域名解析服务申请”进行注册。

服务提供者： 选择提供DDNS的服务器，本路由器内置花生壳DDNS客户端。单击“注册”可以登录花生壳首页进行注册。

用户名、密码： 请正确填写在DDNS上注册的用户名和密码。

启用DDNS： 该项用来启用花生壳DDNS服务。

登录/退出： 点击该按钮，可以登录/退出DDNS服务。

图5-71为注册成功后，用注册的Oray护照和密码登录到DDNS服务器上的连接成功示意图。当连接状态显示成功后，互联网上的其它主机就可以通过域名信息中的域名来访问您的路由器或虚拟服务器了。

提示：

如果希望将局域网中的服务器向互联网开放，则还需要在转发规则功能中设置相应的端口映射。具体设置请参考5.9 转发规则部分。

5.17 系统工具

在**系统工具**中，可以对路由器进行优化配置。

- 系统工具
  - 时间设置
  - 诊断工具
  - 软件升级
  - 恢复出厂设置
  - 备份和载入配置
  - 重启路由器
  - 修改登录口令
  - 系统日志
  - 流量统计

- 时间设置，用于设置当地所在时区，获取准确的网络时间。
- 诊断工具，用来检测路由器与其他网络设备的连接状况。
- 软件升级，用于通过 Web 页面升级路由器的软件版本。
- 恢复出厂设置，用于恢复路由器的出厂默认设置。
- 备份和载入配置，用于备份系统设置信息，并在需要时将其重新载入。
- 重启路由器，用于通过 Web 页面重新启动路由器。
- 修改登录口令，用于修改登录本 Web 页面的用户名和密码，防止非授权人员随意登录 Web 设置页面。
- 系统日志，用于查看系统日志信息以快速定位设备故障或了解网络情况。
- 流量统计，用于实时查看局域网用户通过路由器进行通信的情况。

单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.17.1 时间设置

选择菜单**系统工具→时间设置**，可以在下图 5-72界面中设置路由器的系统时间。设置系统时间有两种方式，手动设置系统时间和通过互联网获取标准的GMT时间。

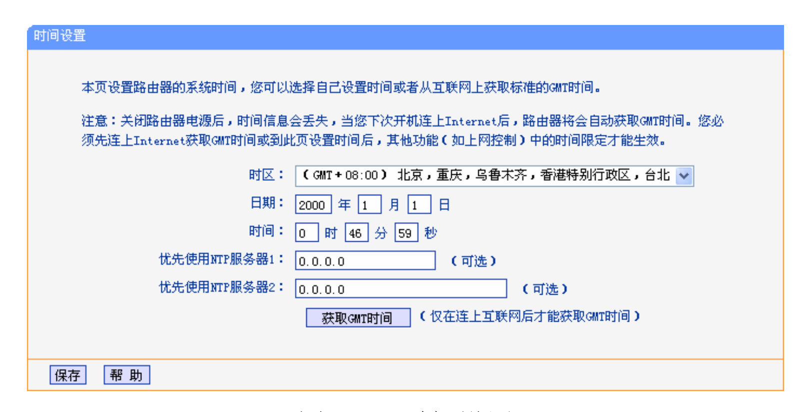


图 5-72 时间设置

优先使用NTP服务器： 该项用来设置NTP服务器的IP地址(最多可以输入两个)。NTP服务器是网络时间服务器，用于同步互联网上的计算机时间。该路由器中内置了一些常用的NTP服务器地址，一旦与Internet连接后，路由器可以自动获取系统时间。但是，若此处设置了该项，则当路由器获取GMT时间时，将优先从已设置的时间服务器上获取。

时间设置方式：

手动设置时间： 首先请选择您所在的时区，然后在日期和时间栏内填入相应值，最后单击**保存**按钮即可完成系统时间的设置。

获取GMT时间： 首先请连接互联网，然后选择您所在的时区，最后单击**获取GMT时间**按钮即可从互联网上获取标准的GMT时间。

☞ 注意：

1. NTP（Network Time Protocol, 网络时间协议）用来为路由器、交换机和工作站之间提供时间同步。时间同步的作用是可以将多台网络设备上的相关事件记录联系起来，有助于分析复杂的故障和安全事件等。
2. 关闭路由器电源后，时间信息会丢失，只有当下次开机连上Internet后，路由器才会自动获取GMT时间。
3. 必须先通过Internet获取GMT时间或在此页手动设置系统时间后，路由器其他功能(如防火墙)中的时间限定才能生效。

5.17.2 诊断工具

选择菜单**系统工具→诊断工具**，可以在下图 5-73界面中通过使用Ping或Tracert功能来测试路由器和其它主机（包括网络设备）的连接情况。

诊断工具

在本页面可以使用ping或者tracert，诊断路由器的连接状态。

参数设置

选择操作： Ping Tracert

IP 地址/域名：

Ping 包数目： 4 （1-50）

Ping 包大小： 64 （4-1472字节）

Ping 超时： 800 （100-2000 毫秒）

Tracert 跳数： 20 （1-30）

诊断结果

路由器已经就绪。

开 始 帮助

图 5-73 诊断工具

选择操作： 选择使用Ping或Tracert功能来检测路由器的连接状态。其中Ping功能用来检测路由器和被测主机是否已连通及连接延时等，而Tracert功能用来检测路由器要连通被测主机时需经过的其他路由器的个数。

IP地址/域名： 与路由器连接的设备的IP地址或域名。

Ping包数目： Ping操作发出的Ping包数目，推荐保持默认值4。

Ping包大小： Ping操作发出的Ping包的大小，推荐保持默认值64。

Ping超时： 设置Ping操作的超时时间。即超过这个时间没收到回应（Reply）时，认为Ping操作失败。

Tracert跳数： 设置Tracert的跳数，即超过此跳数值还没有连通待测设备时，将被判定为连接失败。

填好相关参数后单击**开始**按钮，路由器就开始进行相应的Ping或Tracert测试了，并显示测试结果。

下图5-74是路由器与域名为www.baidu.com的主机正常连接时使用Ping功能诊断的结果，图5-75是路由器与域名为www.baidu.com的主机没有连通时使用Ping功能诊断的结果。



图 5-74 Ping 诊断结果—成功

诊断结果

```
Pinging www.baidu.com [202.108.22.5] with 64 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for www.baidu.com
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

图 5-75 Ping 诊断结果—失败

图 5-76是路由器与IP地址为 10.145.206.66 的主机正常连接时使用Tracert功能诊断的结果，图 5-77是路由器与IP地址为 10.145.206.66 的主机没有连通时使用Tracert功能诊断的结果。



图 5-76 Tracert 诊断结果—成功

诊断结果

```
Tracing route to 10.145.206.66 over a maximum of 20 hops

1    *    *    *      Request timed out.
2    *    *    *      Request timed out.
3    *    *    *      Request timed out.
4    *    *    *      Request timed out.
5    *    *    *      Request timed out.
6    *    *    *      Request timed out.
7    *    *    *      Request timed out.
8    *    *    *      Request timed out.
9    *    *    *      Request timed out.
```

图 5-77 Tracert 诊断结果—失败

5.17.3 软件升级

选择菜单**系统工具→软件升级**，可以在下图 5-78界面中升级本路由器的软件版本以获得更多的功能和更为稳定的性能。

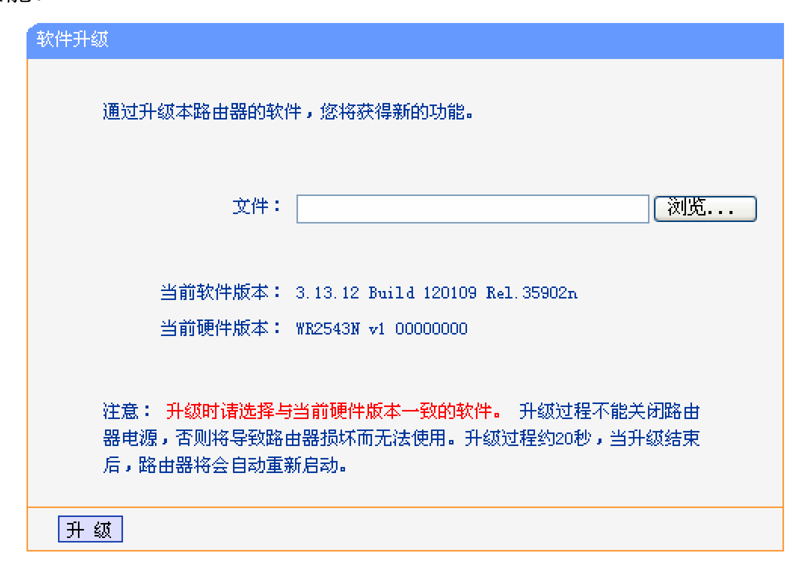


图 5-78 软件升级

软件升级步骤：

第一步：登录本公司的网站(http://www.tp-link.com.cn)，下载最新版本的软件。

第二步：点击**浏览**按钮选择下载的文件，或在"文件"栏内填入已下载升级软件文件的全路径文件名。

第三步：单击**升级**进行软件升级。

第四步：升级完成后，路由器将自动重启。

☞ 注意：

1. 升级软件后，路由器可能会恢复到出厂默认设置，现有的所有设置信息将丢失，建议在升级软件之前备份现有设置信息。
2. 升级时请选择与当前硬件版本一致的软件。升级过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。当升级结束后，路由器将会自动重启。

5.17.4 恢复出厂设置

选择菜单**系统工具→恢复出厂设置**，可以将路由器的所有设置恢复到出厂时的默认状态。恢复出厂设置后，路由器将自动重启，恢复出厂设置页面如图 5-79。

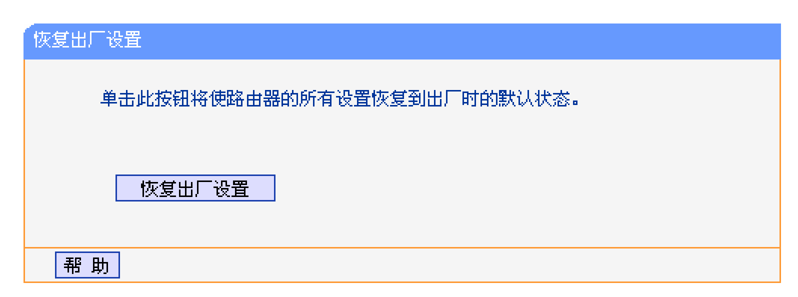


图 5-79 恢复出厂设置

单击**恢复出厂设置**按钮，路由器的所有设置将恢复到出厂时的默认状态。其中：

- 默认的用户名：admin
- 默认的密码：admin
- 默认的IP地址：192.168.1.1
- 默认的子网掩码：255.255.255.0

☞ 注意：

请在恢复出厂设置前备份配置信息。若有需要则可通过载入备份的配置信息来恢复路由器的配置。

5.17.5 备份和载入配置

选择菜单**系统工具→备份和载入配置**，可以在下图 5-80中备份或载入路由器配置文件。

配置备份功能可以将路由器的设置以文件形式保存到电脑中，以备下次使用；在升级路由器软件或在载入新的配置文件前备份路由器的原有配置，可以有效防止升级软件或载入新配置文件过程中丢失原有配置的问题。

配置载入功能则可以将先前保存的或已编辑好的配置文件重新载入。

如果需要为多台路由器配置相同的设置，则可以先配置一台路由器，保存其配置文件后，再将其载入到其它的路由器中，这样可以有效节省配置时间。

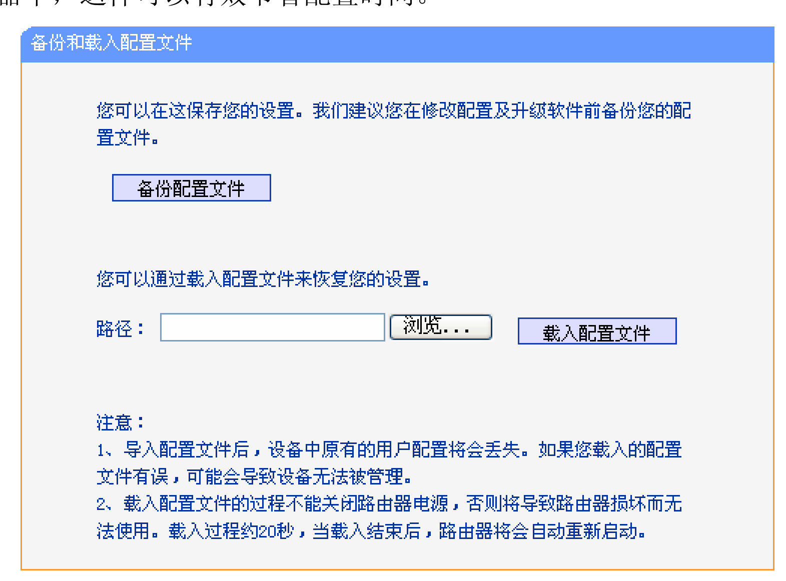


图 5-80 配置文件备份与载入

例1：如果您希望备份现有路由器的配置文件到C:\Router\backup，请按照如下步骤操作：

1. 在图 5-80界面中点击**备份配置文件**。

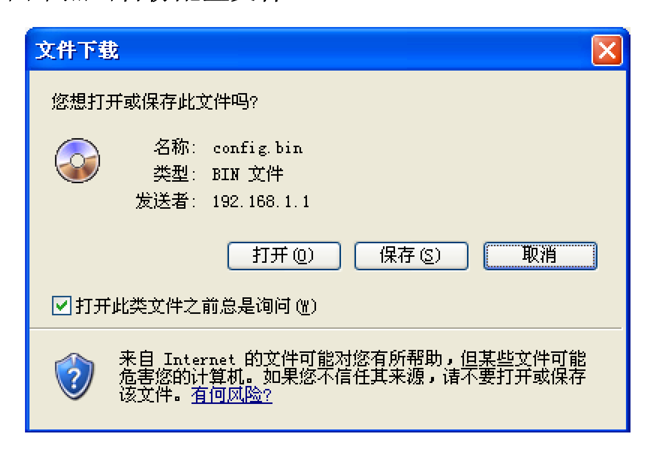


图 5-81 备份配置文件-文件下载

2. 在图 5-81界面中点击**保存**按钮。

3. 在图 5-82界面中选择文件存放路径"C:\Router\backup"，然后点击**保存**按钮即可完成文件备份。

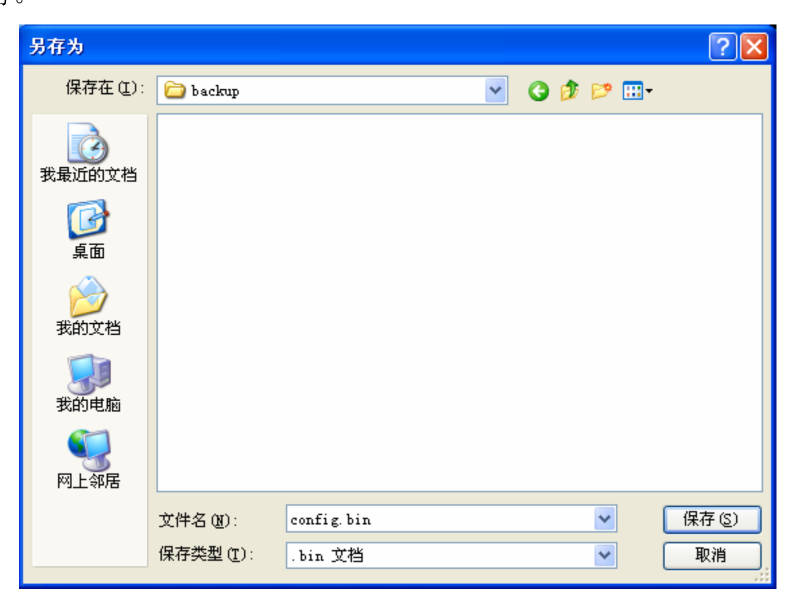


图 5-82 备份配置文件-选择文件存放路径

例2：如果您希望将C:\Router\backup目录下的config.bin文件载入到路由器中，请按照如下步骤操作：

1. 在图 5-80界面中单击**浏览**按钮来选定config.bin文件，或者在"路径"栏中输入文件的全路径"C:\Router\backup\config.bin"。

2. 在图 5-80界面中点击**载入配置文件**按钮即可。

☞ 注意：

1. 载入配置文件后，设备中原有的配置信息将会丢失，所以在导入配置文件前请先备份配置。如果载入的配置文件有误，可重新载入先前备份的文件。
2. 配置文件载入的过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。载入文件的大小及配置命令正确与否会影响载入过程所需要的时间。如果载入结束且没有错误，路由器将会自动重新启动。如果载入有错，请根据提示信息自己选择是否保存配置，最好能重启路由器。

5.17.6 重启路由器

选择菜单**系统工具→重启路由器**，可以将路由器重新启动，如图 5-83。



图 5-83 重启路由器

本路由器的某些设置需要在路由器重新启动后才能生效。

➢ 设置后系统能自动重启的项目有：
  - 对路由器进行软件升级
  - 恢复路由器的出厂设置
  - 修改 LAN 口的基本网络参数
➢ 设置后需手动重启路由器才能生效的项目有：
  - 设置 WPS 安全设置功能
  - 设置 DHCP 服务功能
  - 设置 DHCP 服务器的静态地址分配功能
  - 设置无线网络的基本参数
  - 修改无线网络的安全设置
  - 修改无线网络的高级设置
  - 修改路由器的远程 WEB 管理端口

  手动重启的方法：单击图 5-83中的**重启路由器**按钮。

5.17.7 修改登录口令

选择菜单**系统工具→修改登录口令**，可以在下图 5-84界面中修改登录路由器管理界面的用户名和密码。修改完成后，点击**保存**按钮即可。

修改登录口令

本页修改系统管理员的用户名及口令，用户名及口令长度不能超过14个字节。

原用户名： admin

原口令： ●●●●●

新用户名： User

新口令： ●●●●●●●●●●

确认新口令： ●●●●●●●●●●

保 存 清 空

图 5-84 修改登录口令

☞ 注意：

出于安全考虑，我们强烈推荐您更改初始系统管理员的用户名及密码。如果忘记了系统密码，请将路由器恢复到出厂设置(如何恢复请参考3.2 复位)。

5.17.8 系统日志

选择菜单**系统工具→系统日志**，可以在下图 5-85中查看路由器的日志信息。该界面记录了路由器的系统日志，可以通过查询日志了解网络情况和快速定位设备故障。



索引	时间	类型	级别	日 志 内 容
34	1st day 00:01:41	DHCP	NOTICE	DHCPC DHCP Service unavailable, recv no OFFER
33	1st day 00:01:39	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 1
32	1st day 00:01:37	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 1
31	1st day 00:01:33	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
30	1st day 00:01:31	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
29	1st day 00:01:29	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
28	1st day 00:00:49	DHCP	NOTICE	DHCPC DHCP Service unavailable, recv no OFFER
27	1st day 00:00:47	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 1
26	1st day 00:00:45	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 1
25	1st day 00:00:41	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
24	1st day 00:00:39	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
23	1st day 00:00:37	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
22	1st day 00:00:28	安全	INFO	Wlan weak security warning enables
21	1st day 00:00:27	DHCP	NOTICE	DHCPC DHCP Service unavailable, recv no OFFER
20	1st day 00:00:24	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 1
19	1st day 00:00:22	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 1
18	1st day 00:00:20	DHCP	NOTICE	DHCPS:Send ACK to 192.168.1.100
17	1st day 00:00:20	DHCP	NOTICE	DHCPS:Recv REQUEST from 6C:62:6D:F7:32:44
16	1st day 00:00:20	DHCP	NOTICE	DHCPS:Send OFFER with ip 192.168.1.100
15	1st day 00:00:19	DHCP	NOTICE	DHCPS:Recv DISCOVER from 6C:62:6D:F7:32:44
14	1st day 00:00:18	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
13	1st day 00:00:18	DHCP	NOTICE	DHCPS:Send NAK
12	1st day 00:00:18	DHCP	NOTICE	DHCPS:Recv REQUEST from 6C:62:6D:F7:32:44
11	1st day 00:00:16	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0 and unicast flag 0
10	1st day 00:00:15	安全	INFO	RTSP ALG enabled
9	1st day 00:00:15	安全	INFO	H323 ALG enabled
8	1st day 00:00:15	安全	INFO	TFTP ALG enabled
7	1st day 00:00:15	安全	INFO	FTP ALG enabled
6	1st day 00:00:14	安全	INFO	IPSEC Passthrough enabled
5	1st day 00:00:14	安全	INFO	L2TP Passthrough enabled

图 5-85 系统日志

通过邮件定时发送日志功能： 显示是否已启用通过邮件定时发送日志功能。如果想启用此功能，请点击**邮件发送设置**按钮进行相关信息的设置。

邮件发送设置： 点击此按钮，可以在下图5-86界面中设置发送邮件的相关信息。

选择要查看的日志类型： 通过选择下拉列表中日志的种类，可以让页面只显示该种类的日志。

选择要查看的日志等级： 通过选择下拉列表中日志的等级，可以让页面只显示该等级的日志。

刷新： 点击此按钮，路由器将刷新页面，显示最新的日志列表。

保存所有日志： 点击此按钮，可以将所有日志保存为一个文本文件。

通过邮件发送： 点击此按钮，路由器将根据“邮件发送设置”中的地址和验证信息发送一封包含当前日志的邮件。

清除所有日志： 点击此按钮，路由器中的日志将被永久删除。

邮件发送设置

本页设置邮件的发送，并可通过设置时间表来定时发送包含日志的邮件。

邮件帐户设置

发信邮箱地址： abc@163.com

收信邮箱地址： 123@yahoo.com

SMTP服务器地址： smtp.163.com

☑ 启用验证

用户名： abc@163.com

密码： ●●●●●●●●●●

密码确认： ●●●●●●●●●●

☑ 启用定时自动发送日志功能

◉ 在每天的这个时候发送邮件： 18 时 00 分

○ 每间隔一段时间发送邮件： 48 小时

保 存 返 回 帮 助

图 5-86 邮件发送设置

发信邮箱地址： 发送日志时使用的邮件帐户，路由器通过该帐户发送邮件。

收信邮箱地址： 接收日志邮件的邮箱。

SMTP 服务器地址： 提供 SMTP 服务的服务器地址，各大邮件门户网站均提供该服务器，例如 163 邮箱的 SMTP 服务器地址是 smtp.163.com。如果不清楚该地址，可以登录相关的邮件网站查询帮助页面。

启用验证： 需要用户名/密码登录的邮箱基本上都需要启用验证。

启用定时自动发送日志功能： 启用该功能，在每天特定时间或每隔一段时间路由器可以自动通过邮件发送日志。

完成更改后，点击**保存**按钮。

5.17.9 流量统计

选择菜单**系统工具→流量统计**，可以在下图 5-87中查看路由器的流量信息。单击**刷新**按钮，可以更新流量统计表；单击路由器数据流量统计表中对应条目后的**重置**，可以将该条目当前的流量数据全部清零，并重新开始统计；单击**删除**，可以删除指定的流量统计信息。



图 5-87 流量统计

数据包统计时间间隔： 该数值决定了统计路由器当前流量的时间间隔。

IP 地址： 被统计主机的 IP 地址，此处也会显示该主机的 MAC 地址。

总流量： 该项分别用数据包个数和字节数来统计路由器接收和发送数据的总流量。

当前流量： 该项显示在不同的统计单位下，路由器在数据包统计时间间隔内接收和发送不同数据的总流量。

☞ 注意：

若要查看路由器的流量信息，必须先开启路由器的流量统计功能。如无需流量统计，可以关闭该功能，这样可以提高路由器的数据处理能力。

附录A　FAQ

1.　忘记了登录路由器的用户名和密码怎么办（如何将路由器复位）？

忘记了登录路由器的用户名和密码只能将路由器恢复到出厂默认设置，即复位。在路由器的后面板上有一个标识为 RESET 的按钮，这就是**复位键**。通电状态下按下 RESET 键 5 秒钟，所有指示灯均为灭时松开 RESET 键，复位成功。

注意：复位后路由器默认登录 IP 为 192.168.1.1，默认用户名/密码是 admin/admin。登录时，请确保您的计算机的 IP 地址在 192.168.1.X（X 为 2 到 254 之间的任意整数）网段。

2.　登录不了路由器的管理界面怎么办？

1) 请确保您的计算机连接在路由器的 1/2/3/4 口的其中一个，并且相应指示灯是亮的；

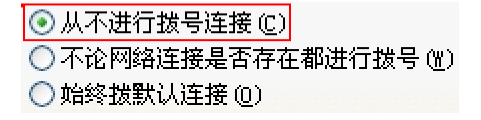
2) 请确认您计算机的 IP 地址与路由器登录 IP 地址处于同一网段；如路由器默认登录 IP 地址为 192.168.1.1，则计算机 IP 地址须为 192.168.1.X（X 为 2 到 254 之间的任意整数）；

3) 如果您修改了路由器的 WEB 管理端口（默认为 80），则登录路由器管理界面时应输入 http://LAN 口 IP:端口号，如 http:192.168.1.1:88；

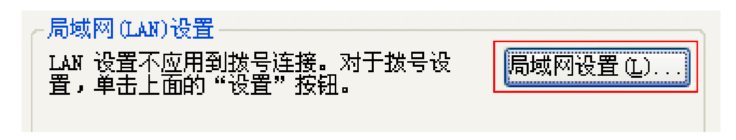
4) 请确保您的浏览器设置为从“不进行拨号连接”并且没有设置代理服务器；

方法如下（以 IE 浏览器为例）：

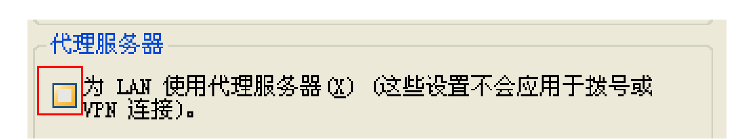
依次选择工具—Internet 选项—连接，选择“从不进行拨号连接”：



单击**局域网设置**



如下图设置：



5) 可尝试更换其它计算机进行登录；

若经过上述操作仍不能登录到路由器，请将路由器恢复出厂设置并重新操作。

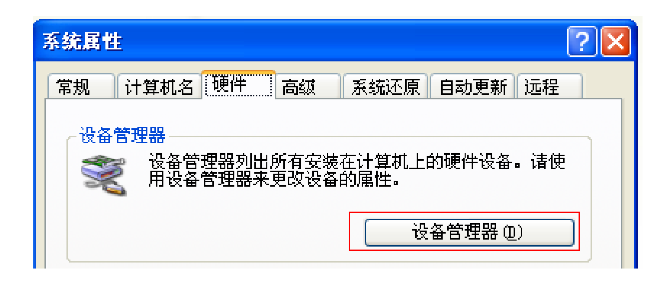
3.　为什么我的笔记本电脑搜索不到无线信号？

1) 如果是笔记本电脑内置的无线网卡，请确认无线功能开关已打开（建议联系笔记本电脑厂商或查阅相关说明书）；

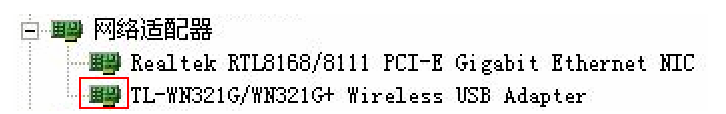
2) 在设备管理器中查看无线网卡驱动是否成功安装以及无线网卡是否已启用；

方法如下：

右键点击桌面上的**我的电脑**，选择**属性-硬件-设备管理器**



如下图中的绿色标识表示网卡驱动已安装成功且启用



3) 检查笔记本电脑的无线服务是否开启；

方法如下（以 Windows XP 为例）：

右键点击桌面上**我的电脑**，选择**管理**。在计算机管理中选择“服务和应用程序”，再在“服务”页面里面查看“Wireless Zero Configuration”的状态

Windows Time	维护在网络上的所有客户端和服务器的时间和...	已启动	自动	本地系统
Wireless Zero Configuration	为您的 802.11 适配器提供自动配置	已启动	手动	本地系统
WMI Performance Adapter	从 WMI HiPerf 提供程序提供性能库信息。		手动	本地系统

4) 请确认您的无线路由器的无线功能已开启且允许 SSID 广播。



5) 请检查您的无线路由器的频段设置是否与您的网卡相匹配。

例如：若您的网卡仅支持 2.4GHz 频段，而您的无线路由器频段却设置在 5GHz，则频段设置与网卡不匹配。

解决方法：请登录路由器设置界面进行如下操作：无线设置→基本设置→频段（选为网卡支持的频段）→保存，重启路由器生效。

6) 尝试近距离是否可以搜索到无线信号，避免因障碍物太多导致信号衰减严重；

如果仍不能搜索到信号，请确认其它的无线网卡是否可以连接到该无线路由器。如果都不可以，请将路由器恢复到出厂设置。

4. 为什么我的笔记本电脑搜到无线信号却连接不上？

1) 请确认尝试连接的无线信号的名称与无线路由器设置的 SSID 号一致；

2) 请确认无线信号的强度，如果信号较弱，建议调整无线路由器的位置或近距离连接；

3) 请确认无线路由器是否设置加密，如果已设置加密，检查无线网卡与无线路由器的加密设置是否一致；

4) 删除您电脑上的无线网卡原有配置文件，重新进行连接；

5) 咨询笔记本电脑或无线网卡的厂商，按照相关的指导操作无线网卡进行连接；

若仍然无法连接，请将路由器恢复到出厂设置并重新设置。

5. 如何判断我的上网方式？

一般情况下，我们可以通过如下几种简单的方法来辨别常见的上网方式：

1) ADSL 虚拟拨号（PPPOE）：宽带服务商只提供了一个用户名和密码（帐号和口令），不接路由器时需拨号上网；

2) 静态 IP 地址：宽带服务商提供了相关的 IP 地址和网关等信息，不用路由器时需要配置相关参数才可以上网；

3) 动态 IP 地址：宽带服务商没有提供任何参数，计算机不需要做任何设置。

6. 无线路由器当无线AP（无线交换机）使用，怎么设置？

在现有的有线网络中实现无线功能时，可以把无线路由器当作一个无线 AP（无线交换机）使用，设置步骤如下：

1) 登录无线路由器管理界面，更改无线路由器的 LAN 口 IP 地址，避免与内网其它设备冲突；关闭无线路由器的 DHCP 功能并重启；

2) 将无线路由器的 1/2/3/4 任意一口与有线网络中的路由器或交换机有线连接起来；

3) 将网络中的无线网卡连接到无线路由器；

4) 配置无线网卡的网络参数(自动获取或手动配置，手动配置参数与原先使用有线时一致)；

7. 忘记无线加密的密钥怎么办？

一般来说有以下两种方法：

1) 使用网线连接计算机和无线路由器，通过有线的方式登录无线路由器并查看**无线安全设置**的相关参数；

2) 将无线路由器恢复到出厂设置。

8. 有线使用正常，为什么无线上不了网？

一般情况下，如果使用有线连接可以正常上网，那么说明路由器的配置基本上是正常的。可以从下面几个方面排除故障：

1) 检查无线网卡和无线路由器是否连接成功，（即检查用无线方式能否登录路由器管理界面）；

2) 确认连接到了正确的无线路由器（根据 SSID 号判断）；

3) 检查无线网络连接是否配置了正确的 IP 地址、网关和 DNS 服务器地址；

4) 检查一下路由器安全设置中有无设置过滤；

9. 为什么QQ正常，却打不开网页？

1) 检查您的网络连接是否配置了正确的 DNS 服务器地址（可以咨询当地运营商或者登录路

由器的管理界面，在**运行状态—WAN 口状态—DNS 服务器**处查看）；

2) 检查浏览器设置为从不进行拨号连接并且没有设置代理服务器；

3) 更换一个浏览器（如 Firefox）进行访问。

10. 无线信号受哪些因素的影响？

1) 无线局域网采用的是微波传输，微波的最大特点就是绕射能力非常弱。家庭中最主要的障碍物就是墙壁，它不仅阻挡无线信号还能把电磁的能量吸收掉，因此身处在墙后面的无线接收设备只能接到很微弱的信号，或没有收到信号。

2) 微波炉、蓝牙设备、无绳电话、电冰箱等的强大磁场会使无线网络信号受到影响。

3) 如果在无线环境中存在多台无线设备还有可能存在频道冲突，无线信号串扰的问题。

4) 距离无线设备及电缆线路 100 米内的无线电发射塔、电焊机、电车或高压电力变压器等强信号干扰源，也可能会对无线信号或设备产生强干扰。

5) 室外传播时天气情况对无线信号的影响也很大，雷雨天或天气比较阴沉的时候信号衰减比较厉害，晴天里信号能传输的距离会比较远。

11. 如何改善信号传输质量？

1) 为无线路由/AP 选择一个最佳的放置地点。这个放置地点的要求如下：一、位置应偏高一些，以便在较高地方向下辐射，减少障碍物的阻拦，尽量减少信号盲区；二、位置地点选择时应使信号尽量少穿越隔墙，最好使房间中的无线客户端能与无线 AP 可视。

2) 修改频道，减少无线串扰。注意：设置自己无线信号发射频道时也要尽量保证离别人的无线信号频道 5 个以上。

3) 减少居家电器干扰，保证信号畅通无阻。放置无线 AP 时尽量远离上述设备。

4) 如果无线路由/AP 天线是可拆卸的，可以通过更换天线达到增强无线信号的目的。

附录B IE浏览器设置

1 打开 IE 浏览器，选择菜单工具→Internet 选项…，如下图 1 所示。



图 1

2 在 Internet 选项界面中点击“连接”，勾选“从不进行拨号连接”，或将“拨号和虚拟专用网络设置”中的设置内容全部删除(即将下图中的“宽带连接（默认）”删除)，如图 2 示。

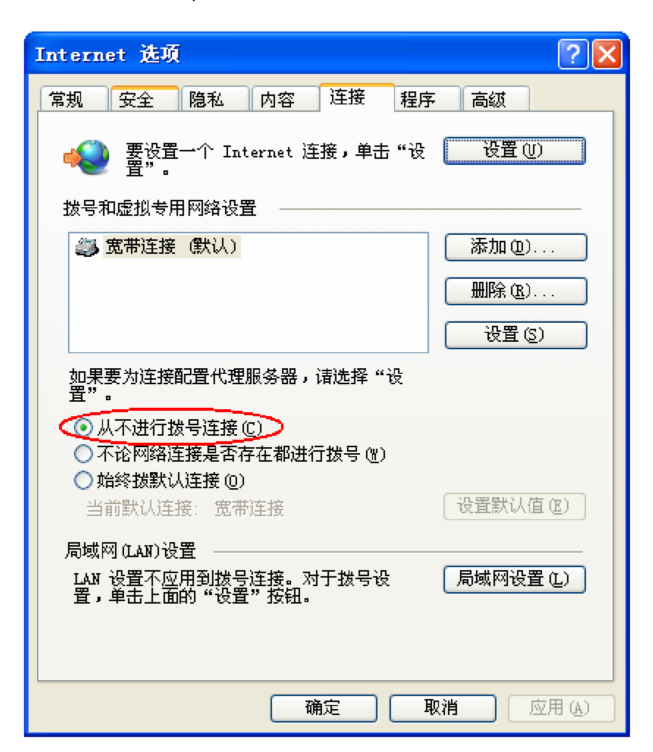


图 2

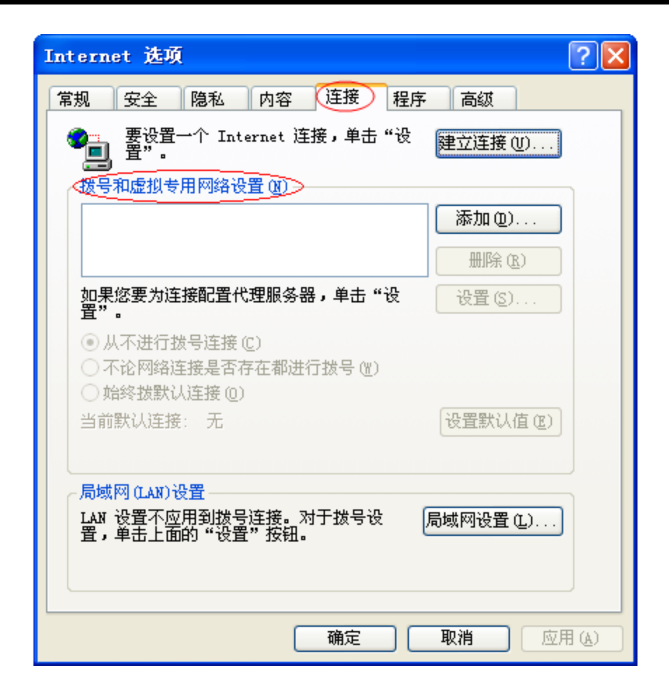


图 3

3　点击图 3 中的**局域网设置…**按钮，确保“代理服务器”下的复选框处于非选中状态，如下图界面所示，单击**确定**按钮返回。

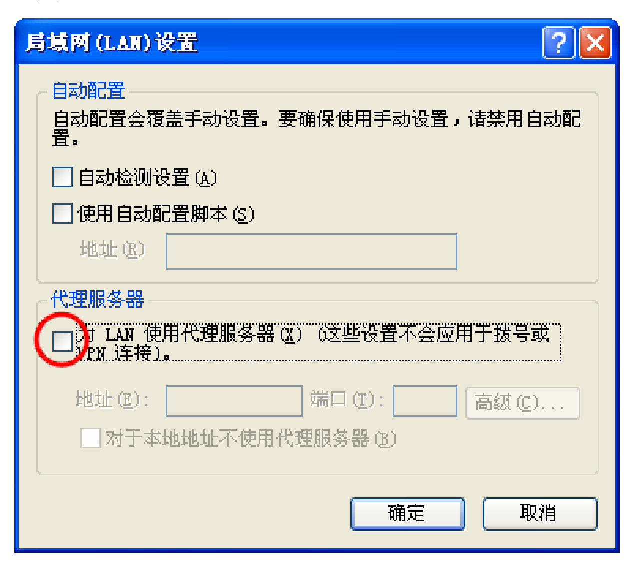


图 4

4　回到 IE 浏览器界面，选择菜单**文件**，单击下拉菜单中的**脱机工作**将该项将前面的“√”去掉，如下图示。若该项前面没有“√”符号则表示脱机工作没有启用，不用设置。

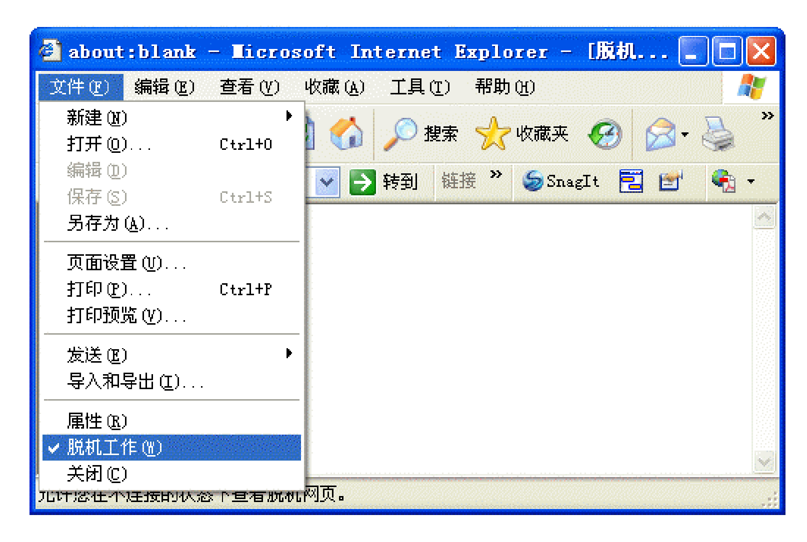
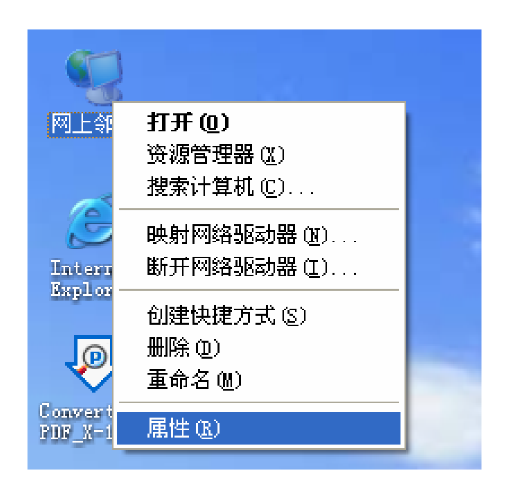

about:blank - Microsoft Internet Explorer - [脱机...
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
新建(N)
打开(O)... Ctrl+O
编辑(D)
保存(S) Ctrl+S
另存为(A)...
页面设置(U)...
打印(P)... Ctrl+P
打印预览(V)...
发送(E)
导入和导出(I)...
属性(R)
脱机工作(W)
关闭(C)
搜索
收藏夹
转到
链接
SnagIt

图 5

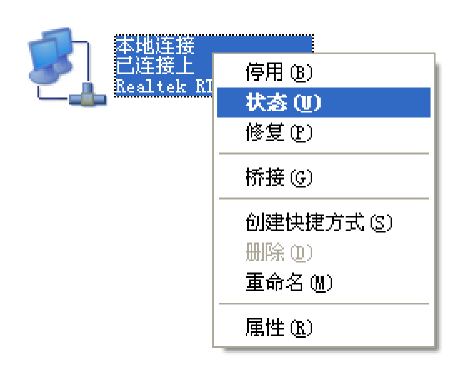
附录C　MAC地址查询

一、Windows XP 系统下的查询

1. 右键单击桌面上的"网上邻居"图标，在弹出的快捷菜单中选择**属性**。



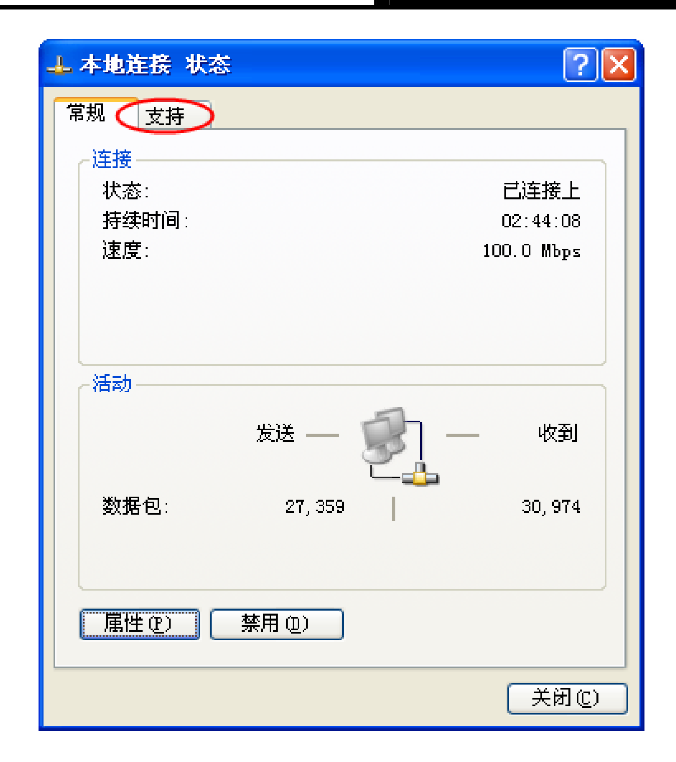
2. 在打开的新页面中，右键单击"本地连接"，选择**状态**。



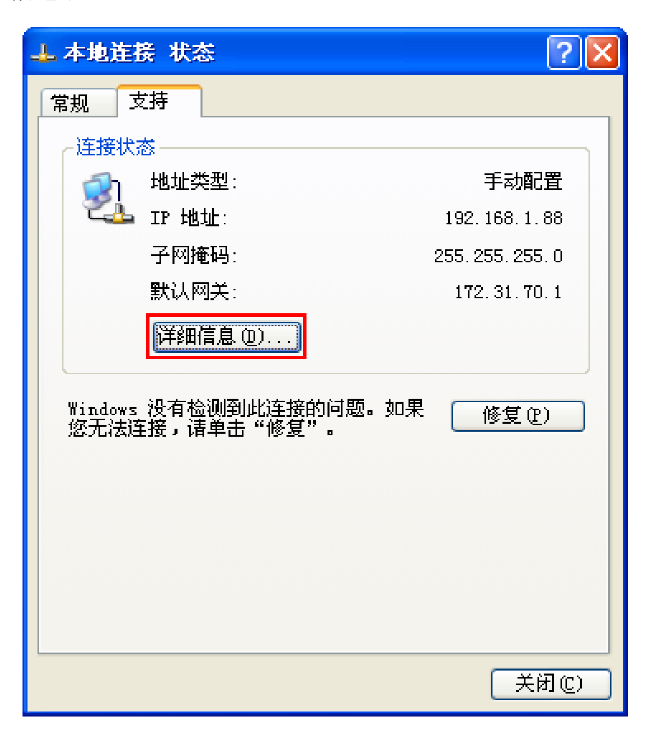
提示：

您也可以在**开始→控制面板→网络和 Internet 连接→网络连接**中找到"本地连接"。

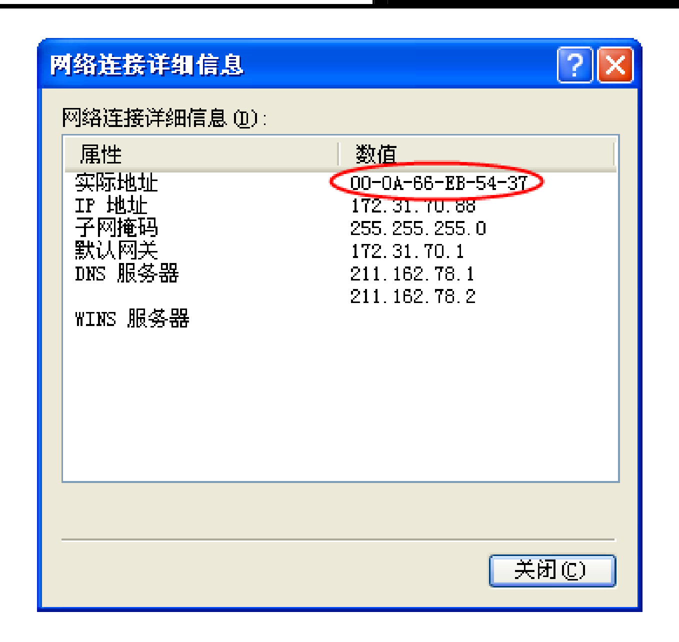
3. 单击"本地连接 状态"页面中的"支持"选项卡。



4. 单击页面中的**详细信息**按钮。



5. 在打开的“网络连接详细信息”页面中，显示的“实际地址”即是当前计算机的 MAC 地址。MAC 地址格式为 XX-XX-XX-XX-XX-XX，其中 X 为 16 进制数，即 0~9 或 A~F 之间的值。此例中查看到的 MAC 地址为 00-0A-66-EB-54-37。

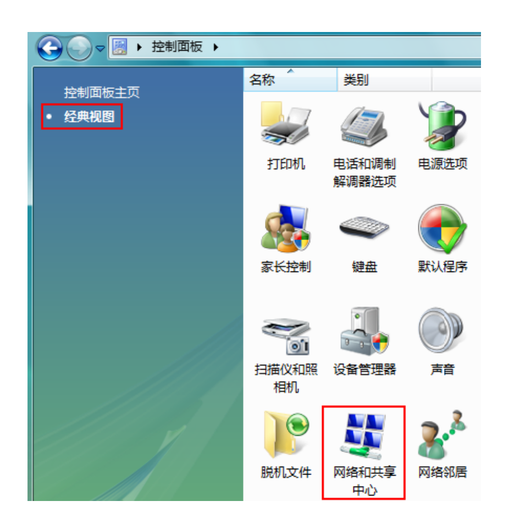


二、Windows Vista 系统下的查询

1. 单击任务栏上的开始按钮，然后选择“控制面板”。



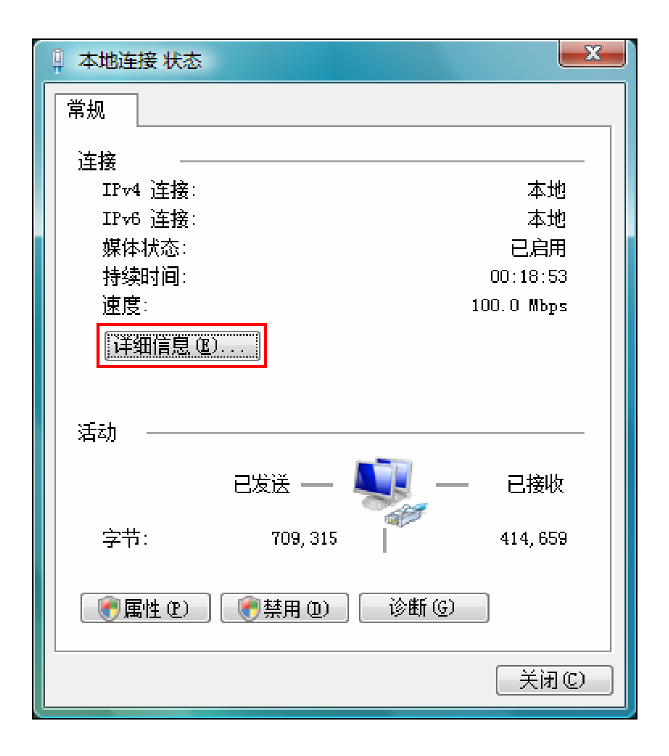
2. 选择页面左边的“经典视图”，然后双击“网络和共享中心”。



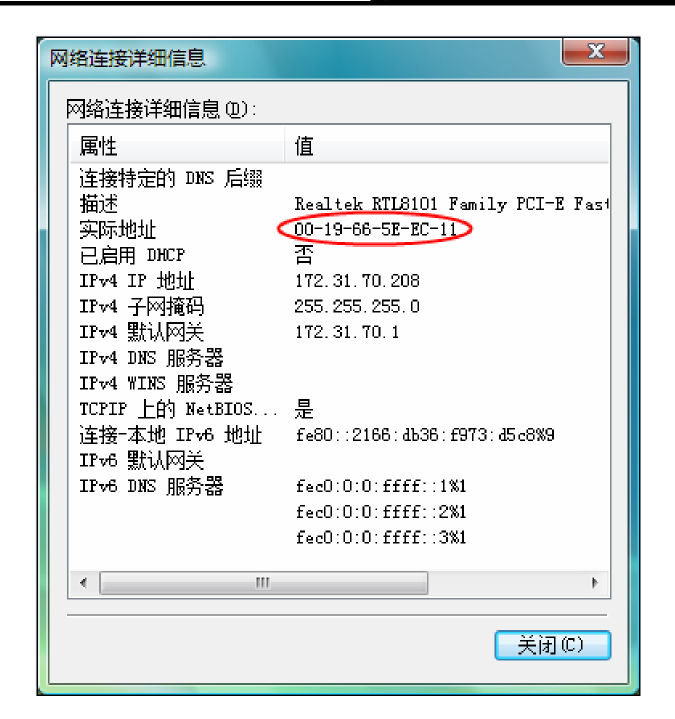
3. 在打开的页面中，单击“查看状态”。



4. 单击“本地连接 状态”页面中的**详细信息**按钮。



5. 在打开的“网络连接详细信息”页面中，显示的“实际地址”即是当前计算机的 MAC 地址。MAC 地址格式为 XX-XX-XX-XX-XX-XX，其中 X 为 16 进制数，即 0~9 或 A~F 之间的值。此例中查看到的 MAC 地址为 00-19-66-5E-EC-11。


网络连接详细信息
网络连接详细信息(D):
属性
值
连接特定的 DNS 后缀
描述
Realtek RTL8101 Family PCI-E Fast
实际地址
00-19-66-5E-EC-11
已启用 DHCP
否
IPv4 IP 地址
172.31.70.208
IPv4 子网掩码
255.255.255.0
IPv4 默认网关
172.31.70.1
IPv4 DNS 服务器
IPv4 WINS 服务器
TCPIP 上的 NetBIOS...
是
连接-本地 IPv6 地址
fe80::2166:db36:f973:d5c8%9
IPv6 默认网关
IPv6 DNS 服务器
fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
关闭(C)

附录D 规格参数

支持的标准和协议		IEEE 802.11a、IEEE 802.11b、IEEE 802.11g、IEEE 802.11n、 IEEE 802.3、IEEE 802.3u、IEEE 802.3x、IEEE 802.14X、CSMA/CA、CSMA/CD、TCP/IP、DHCP、ICMP、NAT、PPPoE
端口	LAN口	4个10/100/1000Mbps自适应RJ45端口(Auto MDI/MDIX)
	INTERNET口	1个10/100/1000Mbps自适应RJ45端口(Auto MDI/MDIX)
	USB口	1个USB 2.0端口
无线参数	频率范围	2.4～2.4835GHz，5.725～5.825GHz
	传输速率	11b：1/2/5.5/11Mbps 11a/g：6/9/12/18/24/36/48/54Mbps 11n：最高可达450Mbps
	工作信道	2.4GHz频段下可选1~13；5GHz频段下可选149、153、157、161、165
	展频技术	DSSS（直接序列展频）
	数据调制方式	11n/g/a：QPSK,BPSK,16-QAM,64-QAM for OFDM 11b：CCK,QPSK,BPSK；
	介质接入协议	CSMA/CA with ACK
	数据加密	WEP；WPA/WPA2；WPA-PSK/WPA2-PSK
	传输功率	20dBm（最大值）
	天线数目	3根
	天线类型	外置可拆卸全向2.4GHz&5GHz双频天线
网络介质.		10Base-T：3类或3类以上UTP
		100Base-TX：5类UTP
		1000Base-T：5类和5类以上UTP
LED指示	端口	(广域网状态指示灯)、1-4(局域网状态指示灯)、(USB状态指示灯)
	其它	(电源指示灯)、2.4GHz(2.4GHz无线状态指示灯)、5GHz（5GHz无线状态指示灯)、（WPS安全连接指示灯）
外形尺寸(L x W x H)		234mmx155mmx36mm
使用环境		工作温度：0ºC 到 40ºC

	存储温度：-40ºC 到 80ºC
	工作湿度：10% 到 90% RH不凝结
	存储湿度：5% 到 90% RH不凝结